Military Intelligence
PROFESSIONAL BULLETIN

January-March 1997
PB 34-97-1

Information Operations

FROM THE EDITOR

Greetings from the home of Military Intelligence! As the Army enters the Information Age, it faces many opportunities **and** many obstacles. This edition of the ***Military Intelligence Professional Bulletin*** offers some excellent observations on information operations (IO) and how the intelligence community will face and overcome these challenges. Major General Thomas in Vantage Point addresses information dominance as the key to IO, and stresses the importance of MI in achieving it. Our feature articles discuss battlefield visualization, IO execution, information threats, and the application of power in the 21st century. A list of some books recommended for lieutenants' professional development is on page 54.

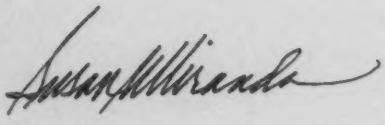
In this issue, we have added a new department: Combat Training Center Notes. Let us know what you think—if there is a topic that you feel needs to be discussed, write us here at ***MIPB***, call, or E-mail us. We are always open to suggestion.

Due to the overwhelming response from our readers, ***MIPB*** is publishing the revised Key Intelligence Personnel Roster and local points of contact; it is in the center of the magazine. Our intent is to provide the field with a handy reference for hard-to-find numbers within the MI Corps. We plan to publish this helpful document each January.

We are always seeking articles. You may write about any topic that may be of interest to our readers. We always welcome articles from our sister Services and allied nations too. Upcoming issues will cover—

- ☐ More articles on Bosnia and support to or lessons learned from Operation JOINT ENDEAVOR and Zaire.
- ☐ Situational awareness.
- ☐ Tactical-level unit training, crew drills, unit standard operating procedures, "how to" tips and hints, and lessons learned from CTC rotations.
- ☐ We always accept historical essays, lessons-learned articles (post-Haiti), and "think pieces."

We would like photos too, even without articles. Be sure to include your name, address, telephone number, and the photographer's full name. Please send caption for the photos with the names of persons, activities, and systems depicted. (Photographers would get a copy of the magazine.)



Writer of the Quarter

MIPB is pleased to announce that Captain Harry E. Jones is our **Writer of the Quarter** (January-March 1997) for the article, "Information Dominance for Army XXI: Battlefield Visualization." Congratulations to Captain Jones, and many thanks to all of our authors for their great articles, book reviews, and letters to the editor. Contributions like yours make ***MIPB*** the professional forum for MI professionals.

How to Submit an Article to MIPB

1. Select a relevant topic of interest to the MI community.
2. Write an outline to organize your work. Put the bottom line up front and write clear, concise introduction and conclusion paragraphs.
3. Follow proper rules of grammar. Consult **DA Pamphlet 600-67** or William A. McIntosh's **Guide to Effective Writing**, if necessary.
4. Maintain the active voice as much as possible. Write "Congress cut the budget" rather than "the budget was cut by Congress." (See **DA Pamphlet 600-67, Effective Writing for Army Leaders**, paragraph 3-2,b[1].)
5. Send the article to Commander, USAIC&FH, ATTN: ATZS-TDL-B, Fort Huachuca, AZ 85613-6000 or E-mail mirandas@huachuca-emh1.army.mil. Please include with your article—
   - ☐ Pictures, graphics, and crests with an adequate description and photographer credits. (We can return photos if so requested.)
   - ☐ A computer diskette with the article in Microsoft Word, Word Perfect, or ASCII. Please do not use special document templates, and separate any graphics files from the text on the disk.
   - ☐ A release by your local security office stating that your article is unclassified, nonsensitive, and releasable to the public.
   - ☐ A short biography with the full names of all authors of the article. The biography should include each author's current duty position, other related assignments, civilian degrees, and advanced military education (CGSC, War College, SAMS, MSSI, SEIP, PGIP). (Tell us if we can print your telephone number and E-mail address with the biography.)
   - ☐ A cover letter with work, home, and E-mail addresses and telephone numbers, stating your wish to have the article published.
6. Remember, content is the most important part of your article. When in doubt, **send us your article**—we can work out the details.

Military Intelligence

PB 34-97-1
Volume 23 Number 1
January-March 1997

FEATURES

8 **Information Dominance for Army XXI: Battlefield Visualization**
by Captain Harry E. Jones, II

11 **Information War: Rethinking the Application of Power in the 21st Century**
by Douglas H. Dearth

17 **U.S. Army Information Operations: Concept and Execution**
by Captain James E. McConville, USAR

23 **Land Information Warfare Activity: IO and IW Support to Army XXI**
by Staff Sergeant Richard A. Sizer

25 **Information Warfare: Protecting Force Sustainment**
by Chief Warrant Officer Two Thomas M. Reardon, USA (Retired)

28 **Roster of Key Intelligence Personnel**

31 **Information Warfare: Good News and Bad News**
by Major Keith D. Anthony, USAR

34 **Information Warfare: Malicious Software and Technology**
by David L. Potter

37 **Non-Nuclear EMP: Automating the Military May Prove a Real Threat**
by Major Scot W. Merkle

40 **The Internet: Resource or Quagmire??**
by Chief Warrant Officer Four Alan D. Tompkins, USAR

42 **Owning the Weather: Weather Support to Force XXI**
by Richard J. Szymber

DEPARTMENTS

2 **Vantage Point**
3 **CSM Forum**
5 **Letters**
46 **CTC Notes**
49 **Concepts and Doctrine**
55 **Proponent Notes**
55 **MI Corps Hall of Fame**
56 **Reserve Component**
58 **Professional Reader**
61 **Unit Profile**

STAFF:

Commanding General
Major General Charles W. Thomas

Director of Operations, Training, and Doctrine
Colonel Robert C. White, Jr.

Editor
Captain Susan M. Miranda

Associate Editor
Elizabeth A. McGovern

Art Director
Private First Class Andy M. Hobbs

Graphics Specialist
Marvin H. Marcroft

Administration
Cruz M. Martinez

Purpose: The U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH) publishes the ***Military Intelligence Professional Bulletin*** quarterly under provisions of **AR 25-30** and the TRADOC Professional Bulletin policy letter. This bulletin disseminates material designed to keep individuals knowledgeable of past, current, and emerging concepts, doctrine, materiel, training, and professional developments within the Military Intelligence Corps.

Submissions: Send manuscripts, letters to the editor, photographs, and any inquiries to: Commander, USAIC&FH, ATTN: ATZS-TDL-B, Fort Huachuca, AZ 85613-6000 or E-mail mirandas@huachuca-emh1.army.mil. For more information, phone (520) 538-1004 or DSN 879-1004.

Subscriptions: Subscription rates are $10.00 per year (Domestic, APO, and FPO) and $12.50 per year (Foreign). Send change of address and subscriptions (see page 22) to Commander, USAIC& FH, ATZS-TDL-B, Fort Huachuca, AZ 85613-6000. ***Keep us informed of your changes of address!*** For further information, phone (520) 538-1015 or DSN 879-1015.

Disclaimer: This publication presents professional information, but the views expressed herein are those of the authors, not the Department of Defense or its elements. The content does not necessarily reflect the official U.S. Army position and does not change or supersede any information in other U.S. Army publications. Use of news items constitutes neither affirmation of their accuracy nor product endorsement. The ***Military Intelligence Professional Bulletin*** reserves the right to edit submitted material.

By Order of the
Secretary of the Army:
DENNIS J. REIMER
General, United States Army
Chief of Staff

Official:
Joel B. Hudson
JOEL B. HUDSON
Acting Administrative Assistant to
the Secretary of the Army 02923

VANTAGE POINT

by Major General Charles W. Thomas

Information Dominance

The degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation in operations short of war, while denying those capabilities to the adversary.

—FM 100-6, Information Operations

This edition of the ***Military Intelligence Professional Bulletin*** is devoted to the subject of information operations (IO). It is important that the Military Intelligence (MI) Corps begin an active dialogue on this rapidly maturing concept. The newly published **FM 100-6, Information Operations**, is a good start, but is essentially a work-in-progress. It remains for **us** to further it on its journey toward meaningful application.

Information Dominance is the Key to IO

I use "**us**" because the most serious application of IO involves the notion of **information dominance**—and the majority of that load is handled in large measure by MI systems, force structure, and subject matter experts. While IO involves integrating everything from traditional command and control warfare (C^2W), to psychological operations (PSYOP), civil affairs (CA), and the global information environment (in addition to intelligence), the holistic reason for this integration is information dominance. A key goal of IO is to gain a knowledge advantage in terms of what you know about an adversary versus what he knows about you. This knowledge delta, effectively exploited, is information dominance.

Information dominance begins with knowledge—first, understanding your own strengths and weaknesses, and second, weighing them against those of your adversary. The larger the delta between the two, the more dominant your capability to overmatch an adversary. "Overmatch" is a relative term and, in knowledge-based warfare, may occur only in specific circumstances. Understanding when circumstances are favorable is, again, understanding when you enjoy the information dominance delta.

The most fundamental requirement for information dominance is knowledge about your adversaries' capabilities and intentions—classic intelligence in every sense of the word. There is no question, though, that other aspects of information dominance are also critical to enhancing this knowledge delta. For example, command and control (C^2) attack is essential to suppress an adversary's ability to develop intelligence about us or to C^2 his forces. And

U.S. Army photo

no aspect of information dominance would work without effective friendly information systems.

MI Support—Essential to Information Dominance

The system of systems that MI brings to warfighting over the whole spectrum of conflict is designed to tilt the information dominance delta in our favor. We do this by collecting, producing, and presenting intelligence; disseminating it; and playing a key role in C^2 attack. MI owns the subject matter experts, the systems, and the capability to integrate it all from national through theater to operational and tactical components. The IO mission is ours to work, even though IO is functionally spread throughout the Army. That is, the proponent for IO is the Combined Arms Center, the Signal Center has the lead for C^2 enable, and PSYOP and CA doctrine rests with the special operations community and..., well, you get the idea.

The integral part of IO remains knowledge—read intelligence and relevant information. The harder of the two, by far, is intelligence because it is usually obtained from uncooperative sources. And our ability to accumulate knowledge about ourselves and our adversaries is what, in turn, enables information dominance. So, while we clearly have a key role to play in information dominance, it is not a wholly mature concept, but one that we must all think about in terms of technical and operational architectures, doctrine, and tactics, techniques, and procedures.

Information dominance is a concept for MI operations in the 21st century—we need to work as a team to perfect it as an integrated part of military operations.

ALWAYS OUT FRONT!

CSM FORUM

by Command Sergeant Major Randolph Hollingsworth

Master Sergeant Robert P. Lopez, from the Fort Huachuca Battle Command Battle Laboratory, will be my guest writer for this issue of the ***Military Intelligence Professional Bulletin***. I ask that you keep this issue in a special place for future reference as this article provides you a view of the future of our MI Corps.

The Fort Huachuca Battle Command Battle Laboratory

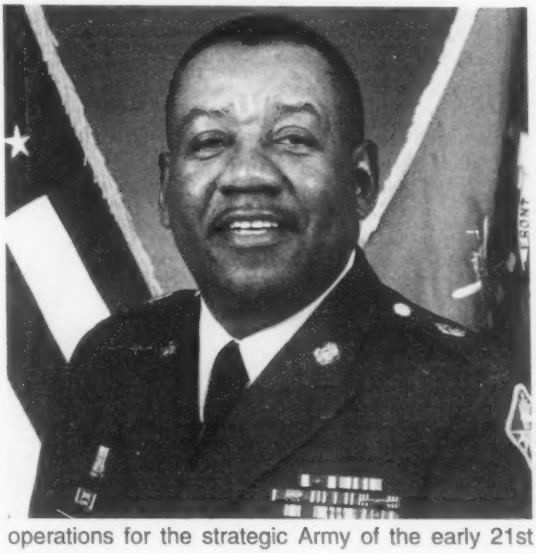
The purpose of this article is to describe the mission of the Fort Huachuca Battle Command Battle Laboratory. Before getting into specifics, let us step back a few years and approach this topic within a historical context.

In 1415, in the middle of a muddy battlefield known as Agincourt, Henry V led 11,000 English pikemen and archers to victory over 51,000 French soldiers. The English longbow was the decisive factor in the decimation of the French knights and helped the English capture Normandy.

In 1588, after braving bad weather along the English Channel, a massive flotilla of Spanish vessels was destroyed by a small fleet of maneuverable English ships equipped with cannons. Naval artillery proved to be the decisive factor in the destruction of the Spanish Armada and marked the beginning of the end of Spanish dominance in Europe.

In June 1950, North Korean troops attacked South Korea and rapidly advanced through the limited maneuver corridors of the Korean peninsula. The inability of the American and South Korean troops to stop the Soviet-made T-34 tank proved to be a decisive factor in the early stages of the Korean War.

Accounts of technologically superior weapons and tactics defeating numerically superior forces using existing doctrine and inferior weapons are as old as war itself. The quest for the 'magic bullet' that can defeat a larger, stronger enemy will continue as long as nations exist. Will the U.S. Army be leading this search for new weapon systems and technologies with military applications? That is the charter of Force XXI: to change the Army to fulfill the needs of the 21st century with the best use of our quality soldiers, leaders, and new technology. As described in **TRADOC Pamphlet 525-5, Force XXI Operations**, this is a concept for the evolution of full-dimensional



U.S. Army photo

operations for the strategic Army of the early 21st century.

Battle Labs conduct various experiments within their respective areas of battle dynamics and focus on battlefield capabilities and priorities. The areas of battle dynamics are—

- ☐ Battlespace (Battlespace Mounted—Fort Knox, Kentucky, and Battlespace Dismounted—Fort Benning, Georgia).
- ☐ Battle command (Fort Leavenworth, Kansas; Fort Gordon, Georgia, and Fort Huachuca, Arizona).
- ☐ Combat service support (Fort Lee, Virginia).
- ☐ Depth and simultaneous attack (Fort Sill, Oklahoma).
- ☐ Early entry lethality and survivability (Fort Monroe, Virginia).

These Battle Labs conduct studies of battlefield capabilities and priorities, leveraging horizontal technology insertion with experimentation to prove new technological advances and rapidly insert them into the Army Force structure.

The focus of Battle Labs is the changing nature of the battlefield. The use of Battle Lab Warfighting Experiments (BLWEs) and Advanced Warfighting Experiments (AWEs) provide the Battle Lab with the freedom to explore, be creative and innovative, and

take advantage of new technological advances. Warfighting experiments pertaining to only one battle dynamic are called BLWEs while those larger experiments centered on several battle dynamics are called AWEs. Both BLWEs and AWEs may use constructive, live, and virtual activity to test the technology or concept.

The current focus of the Battle Command Battle Lab (Huachuca) is the Task Force XXI AWE to be conducted at the National Training Center (NTC), Fort Irwin, California, in March 1997. The integration of enhanced intelligence collection assets into an improved information support architecture will provide the First Brigade, 4th Infantry Division (Mechanized) (4th ID (M)) Experimental Force (EXFOR) commander with a "common, relevant picture of the battlefield" that includes a current enemy situation overlaid on the Blue Force's (friendly units) deployment. The digitalization effort of the Task Force XXI tactical Internet will provide the locations of Blue Force units.

The intelligence community is challenged to deliver timely intelligence developed from all organic, theater, and national assets to the brigade commander. In order to accomplish this, experimentation and validation of these technologies in the field must first occur. Then, incorporation of the validated technologies into the Army force structure will guarantee successful mission accomplishment.

Task Force XXI provides a major test platform for several Advanced Concept Technology Demonstrations (ACTDs) and the field testing of several prototype systems. ACTDs are sponsored and executed jointly by a team comprised of an operational user and a technology developer, with approval and oversight from the Deputy Undersecretary of Defense for Advanced Technology. The Advanced Concept Technology II (ACT II) program enables direct industry involvement, along with Army combat and materiel developers , in helping to define technology that will lead the Army to its Force XXI vision. ACT II supports BLWEs and AWEs through competetive funding of industry's most advanced technologies, prototypes ans non-developmental items.

The Battlefield Awareness and Data Dissemination (BADD) ACTD will deploy and demonstrate an information system to assist the dissemination of data and deliver a consistent picture of the battlefield to warfighters. This is accomplished by the integration of tactical, operational, and national multimedia information, and provides warfighters the ability to receive, manipulate, visualize, and use information.

This demonstration will occur under the strenuous combat-like situation of an NTC rotation. The scenario will be fluid and intense, requiring the EXFOR to relocate ("jump") their Tactical Operation Center (TOC) and its supporting intelligence Analysis Control Team (ACT) several times during the exercise.

Another technological demonstration will be the Semiautomated IMINT (imagery intelligence) Processing (SAIP) System. This technology enables positive identification of moving target indicators and stationary images acquired by reconnaissance and surveillance platforms through automatic target recognition and interactive target recognition technologies.

The Common Ground Station—Prototype (also called CGS-P) will allow the deployed brigade TOC to receive a direct feed from such collection, reconnaissance, and surveillance platforms as the Joint Surveillance Target Attack Radar System (Joint STARS), the Guardrail Common Sensor (GRCS), the TR-1 (U-2) and other theater- and national-level assets. The CGS-P then provides this information to the ACT where a small intelligence element using the prototype All-Source Analysis System—Remote Work Station (ASAS-RWS) will respond to the brigade commander's critical intelligence requirements. As the situation fluctuates, the ACT will be able to provide the Task Force commander with an unparalleled view of the enemy and his deployed equipment.

The Battle Command Battle Lab (Huachuca), in conjunction with the U.S. Army Intelligence Center and Fort Huachuca, has trained 4 ID (M) intelligence soldiers on these prototype systems. Together, they developed tactics, training, and procedures for the employment of these systems. The lessons learned from Task Force XXI will be incorporated into the Division XXI AWE currently planned for November 1997. As commercial technology continues to introduce new software and hardware innovations, it is imperative that the U.S. Army assimilates the best of these technologies and maintains the edge over all potential adversaries.

ALWAYS OUT FRONT!

Master Sergeant Lopez is an Intelligence Analyst currently assigned to the Operations Section of the Battle Command Battle Lab (Huachuca). His previous assignments include: Department of the Army, Military Intelligence Information Management; the Joint Readiness Training Center at Fort Polk, Louisiana; 1st Battlefield Coordination Detachment, Fort Bragg, North Carolina; and many other MI brigade and battalion assignments. He has a bachelor's degree in History from the University of Arizona. Readers can contact him at (520) 533-l888, DSN 821-l888, and through E-mail at lopezr(@ huachuca-emh30.army. mil.

LETTERS

To the Editor:

Lieutenant Colonel Collin A. Agee's article on the Joint Surveillance Target Attack Radar System (Joint STARS) in Bosnia was informative. ["Joint STARS in Bosnia: Too Much Data, Too Little Intel?," ***Military Intelligence Professional Bulletin***, October-December 1996.] In it, he raises some quetions about force structure. This letter is the official response from the Directorate of Combat Developments at Fort Huachuca.

LTC Agee noted that the Modified Table of Organization and Equipment (MTOE) Ground Station Module (GSM) Company at XVIII Airborne Corps was to be deleted. There are discrepencies between what is doctrine and what units are changing as part of their MTOE force. The GSM Company was an MTOE vice a proponent-approved Table of Organization and Equipment (TOE). Joint STARS supports artillery and aviation units as well. Ownership of this targeting resource by the Battlefield Operating Systems (BOSs) that need it will ensure that we do not break faith with the commitments we have made to our fellow soldiers.

LTC Agee also addresses the requirements for the GSM's follow-on, the Common Ground Station (CGS). Both of these systems are intended for the Now Battle---taking perishable data from not only Joint STARS but also the commander's tactical terminal and joint tactical terminal (CTT/JTT), and the unmanned aerial vehicle (UAV) and feeding a product or report to the supported unit. Those same units have the All-Source Analysis System' s Remote Work Station (ASAS RWS) or a complete Analysis and Control Element (ACE). It is the responsibility of these latter elements to develop the common, relevant picture and disseminate it to the warfighter. Currently, there is no requirement to export that picture to the GSM/CGS. We are working on that fix. While the GSM/CGS is evolving, it remains to be seen whether its functions will be limited or training expanded. There are analyst tasks in the current Imagery Ground Station Operator (IGSO) course.

LTC Agee cites the need for an information manager at corps and division. Personnel are not available and any change to the force would have to be offset by a like amount. Rather than reduce intelligence slots, we need to assure personnel assigned to the ACE bring to the job the necessary skills.

Lastly, LTC Agee suggests the Joint STARS squadron be relooked. The applicable TOE 34-534A, Military Intelligence Company (Joint STARS), (297th MI Battalion, 513th MI Brigade) calls for staff personnel as well as command and control. The effective date for this TOE is October 1998. Until then, task organization is the answer.

John K. Quinn
Fort Huachuca, Arizona

To the Editor:

The purpose of this letter is to correct what I perceive to be an error in several recent issues including the April-June issue of the ***Military Intelligence Professional Bulletin***. The error appears in the Editor's Note found on page 43 in the article "Intelligence and the Peacekeeper in Haiti."

The term "Operations Other Than War" used throughout this article is no longer doctrinally accurate. Precise terminology while discussing peacekeeping operations, humanitarian assistance, and operations in aid of civil authorities should replace "OOTW." A message from the Joint Staff, DJS 311514Z Aug 1995 released this guidance.

The term "Military Operations Other Than War (MOOTW)" first appeared in **Joint Pub 3-0**, **Doctrine for Joint Operations**. Since its establishment in **Joint Pub 3-0**, MOOTW has progressively gained wider acceptance and usage; the term was not challenged during the preliminary or final coordination of **Joint Pub 3-07**, **Joint Doctrine for Military Operations Other Than War.** Furthermore, the concept of MOOTW is embedded in other capstone and keystone joint doctrine publications including **Joint Pub 1**, **Joint Warfare of the Armed Forces of the United States**; **Joint Pub 0-2**, **Unified Action Armed Forces**; and **Joint Pub 5-0**, **Doctrine for Planning Joint Operations**.

Subsequent to the approval of **Joint Pub 3-07**, disagreement over the use of the MOOTW framework has surfaced. In spite of recommendations to create a different terminology construct, no adequate substitute has as yet been suggested which better depicts what MOOTW was meant to, and in fact does, convey. "Stability and support operations," "other military operations," and "peacetime operations" are less precise than MOOTW and do not supplant the existing doctrinal framework. Furthermore, deviating from doctrinally approved concepts and definitions, where no "exceptional circumstances" exist, is inconsistent with the established policy for the use of joint doctrine. To do so is in conflict with the Chairman's Title X function of *"Developing doctrine for the joint employment of the armed forces"* and the authoritative-guidance nature of this doctrine.

In my opinion, the intent of the Defense Joint Staff (DJS) message of 31 August 1995 sought to minimize the confusion about the term, not to discontinue the use of an approved and doctrinally

sound term. The message states that—

Military Operations Other Than War is a category for a variety of operations and not an operations itself. There is a clear understanding that some types of military operations other than war can involve combat, presenting commanders and forces with a set of uncertainties with which we previously have not had to cope. In all military communications and correspondence, it is vital to address the specifics of the operation being discussed and not rely on the categorical title of military operations other than war. If peace operations are the topic of a message, use peace operations in the subject line and the text. Improper usage of the term military operations other than war can create confusion and may imply there is a diminished need to provide for the security of U.S./Multinational forces.

Joint Pub 3-07 establishes the Chairman's authoritative guidance for **Joint Doctrine for Military Operations Other Than War**. As the DJS message concludes,

Active discussion of the principles of military operations other than war, particularly where they overlap with and diverge from the principles of war, and the training and planning for them, will help in resolving any confusion that has arisen while this publication was being developed. We request your assistance in this endeavor.

Commander George McCaffrey, USN
Washington, D. C.

*Editor's Note: While the **MIPB** is not intended to be a doctrinal Army reference, it is an approved publication with the mission of professional development. We strive to ensure use of correct doctrinal terminology in the articles published in **MIPB**. According to the final drafts of Army publications **FM 100-20, Stability and Support Operations (SASO)**, dated April 1996, and **FM 101-5-1, Operational Terms and Symbols**, dated July 1996, SASO is the recognized Army term replacing Operations Other Than War (OOTW). Miltary Operations Other Than War (MOOTW) is a term used by the joint community in accordance with **Joint Publication 3-07, Joint Doctrine for Military Operations Other Than War.***

To the Editor:

I appreciate the opportunity to comment on the article ["Victory in Egypt: 3d ID(M) DISE," ***Military Intelligence Professional Bulletin***, October-December 1996] about the 3d Infantry Division (Mechanized) (3d ID(M)) intelligence operations and their good use of a Deployable Intelligence Support Element (DISE). The authors, Lieutenant Colonel Boll, Major Holachek, and Captain Ellington, obviously "have the bubble." It was refreshing to read a precisely correct understanding of current doctrine and the excellent implementation of it that is obviously going on in the 3d ID(M). My reading of how they have used JDISS and INTELINK brought other thoughts to mind that might prove interesting to your readers.

The combination of JDISS and INTELINK provides access to enormous amounts of data through a common "window." In most cases, data linked using hypertext to a server and homepage is accessible to potential users, be they using JDISS applications or a browser application. The power of JDISS is that these systems are in many places where relevant data is analyzed. The standard packages enable a user to "open the window" to another user and get what they have. This is a simple but powerful capability. The JDISS established the paradigm.

The same idea is behind the All-Source Analysis System (ASAS) implementation of browser technology to ride either Analysis and Control Element (ACE) software or remote workstation (RWS) software to enable the surf-and-pull of relevant data by the ASAS intelligence operator-analyst. While recent versions of the ASAS software have put the browser into the systems, the key operational impact will not be realized until the multi-level security (MLS) server and the ASAS Trusted Workstation (TWS) are accredited and fielded to the force. Once fielded, the ACE operator can post all available intelligence from his own echelon (and accessed from higher) to the server and allow any RWS working with TWS to browse all the available information. Furthermore, the capability provided by the TWS to allow the user to establish intelligence requirement profiles will enable the user to tell ASAS and the TWS what areas and entities he is interested in and let the workstation do the monitoring of existing data as it becomes available. This will automatically identify when the "good stuff" shows up. Such a capability at brigade and below can give these echelons a much higher probability of successfully weeding through the volumes of intelligence available to them and finding the nuggets that answer the priority intelligence requirements. The use of a RWS and TWS in the TROJAN Special Purpose Integrated Remote Intelligence Terminal (SPIRIT), as explained by the 3d ID(M) authors, might be the perfect place to incorporate this capability.

The realization of another important requirement—to fully integrate all necessary JDISS 2.0 applications into the ASAS Block II software—will complete a greatly needed capability. In essence, the entire ACE will become a virtual JDISS workstation. Other JDISS users will look through their windows to data in an ACE in the same way that they open a window to another JDISS today. Likewise, this ACE will "see" and be able to work seamlessly with any stand-alone JDISS.

These two powerful capabilities of the future will build upon the methodologies and architectures being used by the 3d ID(M) and other units. Used together, they can more effectively address the need to seamlessly supplement the outputs of national intelligence producers with the particular and much more focused needs of the tactical commander. The trick is to get it done **now**!

Colonel Theodore G. Chopin,
TRADOC System Manager ASAS
Fort Huachuca, Arizona

To The Editor:

Dr. Robert J. Bunker's article ["Internetted Structures and C2 Nodes," ***Military Intelligence Professional Bulletin,*** April-June 1996] makes a fair theoretical argument as to why future armies with nonhierarchical command structures will be more difficult to defeat simply because, if I may use any elementary analogy, "cutting the head off no longer kills the snake." But this relates to the center of gravity concept **only if the center of gravity is command and control (C^2)**.

For example, he states that striking *"the center of gravity of a hierarchical structure can paralyze its decisionmaking capability..."* but would *"have almost no effect on a nonhierarchical structure."* First, this assumes the center of gravity **is** the command structure. Secondly, he misses the point that information is a tool only. Also, while it may fundamentally alter how we communicate, it will not replace the requirement for structured command that is not only fundamental to the very nature of military orders execution, but required for coordinated and synchronized military operation.

In fact, the information age may have the exact reverse effect of the nonhierarchical trend Dr. Bunker predicts. For example, 20 years ago it was not uncommon for a division G3 planner to sit down and write an entire division contingency operations plan, done as a project over a 6-month period with little or no staff interaction. As any division planner who has spent weeks participating in Battle Management Center planning cells will tell you, that would be unthinkable today. This is simply because the overload of information requires much more detailed planning and cooperative mission analysis among battlefield operating system (BOS) staff elements. In this case, information has contributed to a **more** structured hierarchy, due to increased dependence, reliance, and interaction with other staff elements.

Dr. Bunker rightly seems to acknowledge that center of gravity may not just mean C^2, for he states that—

> *...development of internetted structures is likely within societal organizations. Isolating national will, public opinion, or even key individuals as a likely center of gravity will no longer be feasible.*

Perhaps I am missing something, but I do not understand, nor does he argue how, "internetted structures" will bring about a weakened, noncohesive national will, or fragmented public opinion, against a perceived common threat.

Next, if for example, we are facing an enemy whose center of gravity is his artillery forces, I fail to see how his possible complex internetted structure will prohibit us from identifying this as a center of gravity or from successfully defeating this center of gravity. How does this structure eliminate his artillery as a center of gravity? I certainly agree with his assessment that an enemy's *"advanced battle command structure"* will make it more difficult to defeat him. To jump to the conclusion that this somehow eliminates a specific center of gravity makes no sense to me, especially when dealing with "physical strength," a potential component of center of gravity per **FM 100-5, Operations**.

I accept Dr. Bunker's encouragement for junior officers such as myself to take a risk in writings and actively participate in new doctrinal concepts. But Captains Neidrauer and Bennett were not defending an outdated concept when they articulated the center of gravity concept at the lower echelon maneuver level. Down here in tactical units such as the 82d Airborne where "the rubber meets the road" and where most junior officers operate, maneuver commanders want S2s who can identify enemy strengths and weaknesses, and the enemy's center of gravity. They may then employ a defeat mechanism to achieve victory. Until the time centers of gravity may no longer exist, maneuver S2s such as myself must be proficient in their identification and articulation.

Captain Paul T. Carter
Fort Bragg, North Carolina

To the Editor:

Captain Jeffrey Steel made an outstanding point about where an aviation S2 belongs during the battle ["Apache S2: Improving Intelligence Support to Combat Aviation," ***Military Intelligence Professional Bulletin*** January-March 1996]. The **only place** for an aviation unit S2 to be during tactical operations is in the Air Tactical Command Post (ATAC). Having served as the 82d Aviation Brigade S2, I can tell you this is true for three primary reasons.

The distances involved in a deep attack or air assault generally prevent direct communications over the operations and intelligence (O&I) net (FM radio). Sitting back at the command post (CP) in the rear monitoring the dead O&I net is not productive. If you want to influence the current battle, you must be able to talk to the aircraft.

Once an aviation operation is underway, all communications are generally passed over the command net (that is reality). Even the S3 shop in the rear is relatively quiet once an operation begins and the aircraft go across the forward line of own troops (FLOT).

Credibility in any S2 job is critical. Lead from the front. Pilots no-

(Continued on page 60)

Information Dominance for Army XXI: Battlefield Visualization

by Captain Harry E. Jones, II

I want to fight the enemy deep. We need to leverage our technologies to see, target and destroy the enemy when he is far from the FLOT—and when the remaining elements close, it should be a foregone conclusion we will win the close fight, with minimal casualities. Focused intelligence, precision strike, and dominant maneuver are keys to success.

—Lieutenant General John M. Keane, Commanding General, XVIII Airborne Corps

America's Army is in the midst of a remarkable change—change driven by information age technologies that will forever alter the way we fight. Let's take a look at a future battle vignette.

Southwest Asia, December 2005: ARFOR "Movement to Strike"

While the U.S. Army Force (ARFOR) moves quickly across the sands, the commander stares at a large, flat panel display depicting his area of operations. Two armor-heavy mobile strike forces are moving abreast, 30 kilometers ahead, their combat vehicle positions depicted on the display. Windowed in a corner of the display is a logistics screen from the Combat Service Support Control System, showing the force's status by critical classes of supply. Windowed in below that is a live video feed from an Outrider unmanned aerial vehicle (UAV) orbiting 50 km ahead. A red icon blinks on the flat panel display—an intelligence sensor has detected an enemy force ahead. *"Two, zoom in on that—I want to see what they're up to."*

The S2 clicks on the zoom button and the enemy element is quickly portrayed in a high-fidelity, three-dimensional (3D) virtual rendition of the battlespace 50 km ahead. The high-resolution view of the terrain indicates a small valley through which the enemy will have to move—perfect killing ground. Simultaneously, the Analysis and Control Team dynamically retasks the UAV to orient its sensor on the threat. An automatic target recognition (ATR) algorithm in the acquiring sensor's preprocessor indicates T-90 tanks and BMP-3 infantry fighting vehicles. *"S2—assessment?"* barks the commander. *"Sir, lead element of an advanced guard battalion—remainder of the battalion is probably 30 minutes behind this force, and the parent regiment 45 minutes to an hour behind them."*

"S3, net call, bring the strike force commanders up on video. I want to do a white-board drill and use that valley to establish an engagement area." With the strike commanders up on a video teleconference, the commander, S3, S2, and Fire Support Officer (FSO) quickly outline a hasty attack fragmentary order (FRAGO) using a John Madden-style "white-board" application on the Maneuver Control System (MCS). The commander outlines his plan, and adjusts boundaries and attack axes to fit the terrain. The S2 quickly refines the probable enemy course of action (COA) based on the raw intelligence while the S3 completes and issues the warning order digitally to the task force (TF). The FSO and Air Liaison Officer request long-range fires and close air support to attack the regimental main body and second echelon forces. Using the S2's refined template, the TF staff quickly wargames the plan. Satisfied with the plan, the commander directs a TF rehearsal of the execution engagement area using the 3D view of the terrain. An artificial intelligence application indicates a proposed support-by-fire position should be moved to optimize the terrain advantage; the S3 modifies the FRAGO accordingly and issues it digitally across the force.

Realizing he has a situational awareness advantage over the oncoming enemy, the commander requests the general support MI unit to degrade the enemy's communications. At the same time, two Comanche helicopters engage and destroy the enemy's reconnaissance elements. Minutes later, the mobile strike forces attack the enemy battalion from the flanks while Army tactical missile fire begins to attrit the follow-on regiment. In his burning command vehicle, the enemy battalion commander is completely dumbfounded—he is under attack from a force he could not see, could not track, and could not engage beyond direct-fire range.

Battlefield Visualization

Far-fetched? Perhaps not. Many of these capabilities addressed in the vignette are in development under the auspices of the Army's Battlefield Visualization Initiative, now under way at Fort Bragg, North Carolina, and Fort Hood, Texas. Though still in its infancy, the development of battlefield visualization (BV) applications, and their subsequent migration to the Army Battle Command System (ABCS), will forever change the way America's Army trains, plans, wargames, and executes missions across the operational continuum.

Despite much recent attention on the subject of BV, it is not a new concept. On the contrary, the ability to visualize the battlefield has existed since humankind first engaged in conflict. The U.S. Army Training and Doctrine Command's **TRADOC PAM 525-70, Battlefield Visualization**, defines BV as—

the process whereby the commander develops a clear understanding of his current state with relation to the enemy and the environment, envisions a desired end state, and then subsequently visualizes the sequence of activity

that will move his force from its current state to the end state.[1]

Implicit in this is an understanding of the terrain, the current location of friendly and enemy forces, the effects of weather, and the enemy commander's available COAs. BV, therefore, is both an art and a science—the art of battle command, enabled by science and technology to gain and maintain the advantage over an opponent. BV is far more than intelligence—it applies to and must integrate data from every battlefield operating system. While the BV system cannot completely clear the fog of battle, it can empower commanders and their staffs to operate consistently inside the enemy's decision cycle, keeping the opposing commander off balance.

Throughout history, the very best commanders have been able to mentally visualize their battlefields. Based on training, experience, and warfighting intuition, they understand the terrain, how the weather will impact their fight, and how the enemy commander will present his force. Brigadier General John Buford clearly had the ability to visualize his battlefield in the opening hours at Gettysburg. General of the Army Douglas MacArthur at Inchon had the same clarity of vision—again, in his mind's eye. These were exceptional commanders. As we approach the 21st century, however, technology will allow us to empower all commanders with the ability to visualize their battlefields, and to see battles in areas not yet occupied. Coupled with the degradation of the enemy commander's ability to visualize his battlefield through lethal and non-lethal attack and deception operations, we can truly gain ***information dominance*** at critical times and places on the battlefield. This dominance will enable a smaller force to rapidly overwhelm a larger foe, and allow a single brigade to enforce an extended zone of separation or to conduct humanitarian relief operations across a distributed, compartmentalized "battlefield."

Key Technologies

We require the integration of seven key technology areas (see Figure 1) to refine and mature our BV capability: displays, both large flat panels to replace the wooden map boards in our tactical operations centers, and private "heads-up" or retinal displays for individual fighting vehicles, aircraft, and soldiers. BV requires accurate sensors to collect enemy force activity and friendly force locations. We need broad bandwidth networks to rapidly move data across the battlespace. BV also requires extensive databases, including high-resolution digital terrain elevation and features data, entity level simulations, and 3D environments. Computer hardware and software provide the technological engine for most BV applications. Finally, BV requires an ATR automatic target recognition capability to speed the analysis and identification of objects in the battlespace, to speed sensor-to-shooter links, and to decrease the risk of fratricide. TRADOC's Program Integration Offices for Army Battle Command (TPIO-ABCS) and terrain are central to the synchronization of activities across these technology areas.

We are making great progress in each of these areas. Due to the superb efforts of the soldiers of the XVIII Airborne Corps, 4th Infantry Division (Mechanized), and the Experimental Force (EXFOR), Communications and Electronics Command (CECOM), National Reconnaissance Office (NRO), Joint Precision Strike Demonstration, Topographic Engineering Center, TRADOC, and many others, the Army is rapidly prototyping a BV capability.

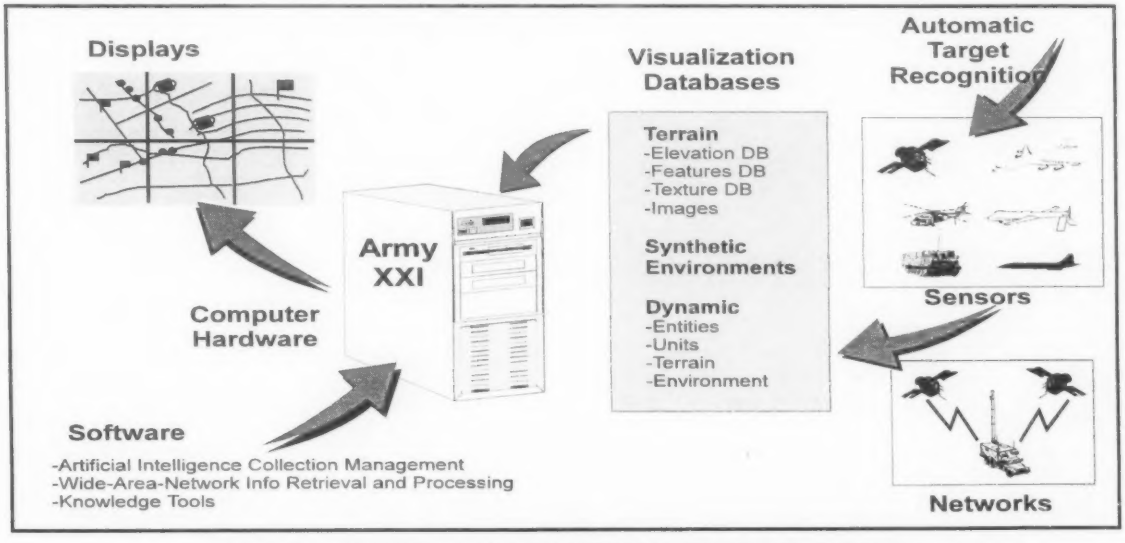


Figure 1. integration of Key Battlefield Visualization Technology.

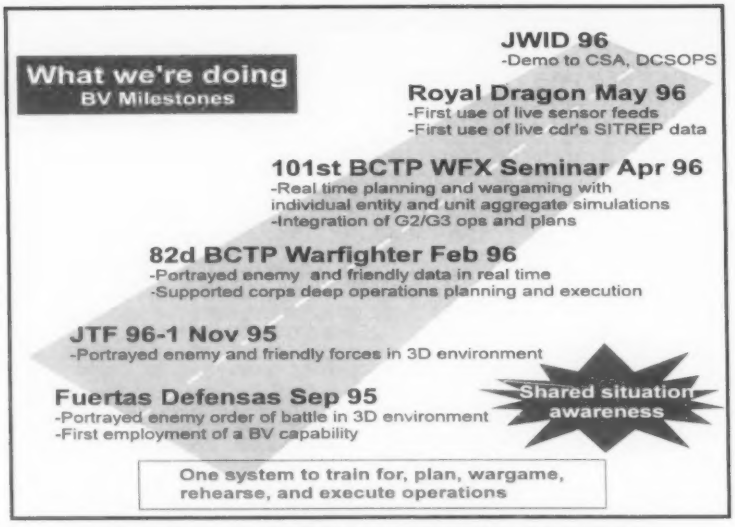

What we're doing
BV Milestones
JWID 96
-Demo to CSA, DCSOPS
Royal Dragon May 96
-First use of live sensor feeds
-First use of live cdr's SITREP data
101st BCTP WFX Seminar Apr 96
-Real time planning and wargaming with individual entity and unit aggregate simulations
-Integration of G2/G3 ops and plans
82d BCTP Warfighter Feb 96
-Portrayed enemy and friendly data in real time
-Supported corps deep operations planning and execution
JTF 96-1 Nov 95
-Portrayed enemy and friendly forces in 3D environment
Fuertas Defensas Sep 95
-Portrayed enemy order of battle in 3D environment
-First employment of a BV capability
Shared situation awareness
One system to train for, plan, wargame, rehearse, and execute operations

Figure 2. Army Battlefield Visualization Milestones.

The Army's BV initiative began in Panama in September 1995 in an exercise called Fuertas Defensas. The NRO provided imagery from national systems to produce high-resolution digital terrain data of a portion of the XVIII Airborne Corps' "exercise box." The Corps intelligence team then overlaid the enemy situation data on the 3D terrain data so the commander could see the fight in a high-resolution, 3D view of the battlespace.

During Exercise Joint Task Force (JTF) 96-1 at Fort Bragg in November 1995, the NRO again provided national systems support to produce digital terrain data of a larger exercise area. Based on feedback from Exercise Fuertas Defensas after-action reviews, the Corps intelligence team added the capability to overlay red and blue data as well as mission planning and rehearsal capabilities. The wooden map boards and paper maps were replaced by two six-foot by eight-foot displays, which provided the commander's "window to the world."

During the 82d Airborne Division's Battle Command Training Program (BCTP) Warfighter exercise at Fort Bragg in February 1996, the prototype BV system—linked with the All-Source Analysis System and the MCS—was fully integrated into the Corps Deep Operations Coordination Cell (DOCC). The BV system portrayed enemy and friendly data in real or near-real time in a 3D, high-fidelity, virtual battlespace replication in support of corps deep operations planning and execution. Using modular semi-automated forces (ModSAF) software which moved enemy units independently, the Corps' planners wargamed against multiple enemy COAs to drive development of branches and sequels.

In XVIII Airborne Corps JTF Exercise Royal Dragon in May 1996, the Corps intelligence team incorporated live sensor feeds for the first time. Air Force U2-R and Army Guardrail Common Sensor and OV-1D Mohawk aerial sensors down-linked through their preprocessors to the BV system. The long-range surveillance unit teams passed spot reports via satellite communications into the ABCS architecture which fed the BV system. Additionally, Grenadier beyond line-of-sight reporting (BRAT) emitters provided real-time updates of friendly force locations. The real-time overlay of red and blue data in a 3D view of the battlespace provided Royal Dragon warfighters with a high-fidelity, virtual view of their fight.

Finally, during the Joint Warrior Interoperability Demonstration (JWID) in August 1996, the BV capability was demonstrated to Army senior leadership. In October, Joint Precision Strike Demonstration's Rapid Battlefield Visualization Advanced Concept Technology Demonstration (RBV ACTD) began. This is a $56 million dollar ACTD that will provide high-resolution digital terrain and features data which are the cornerstone of the BV initiative. The RBV ACTD will also leverage the efforts of CECOM's Battlespace Command and Control Advanced Technology Demonstration (BC^2 ATD). This ACTD has produced a BV workstation that is interoperable with existing ABCS, the Army Global Command and Control System (AGCCS), that uses high-resolution terrain and features data to provide a 3D view of the battlespace.

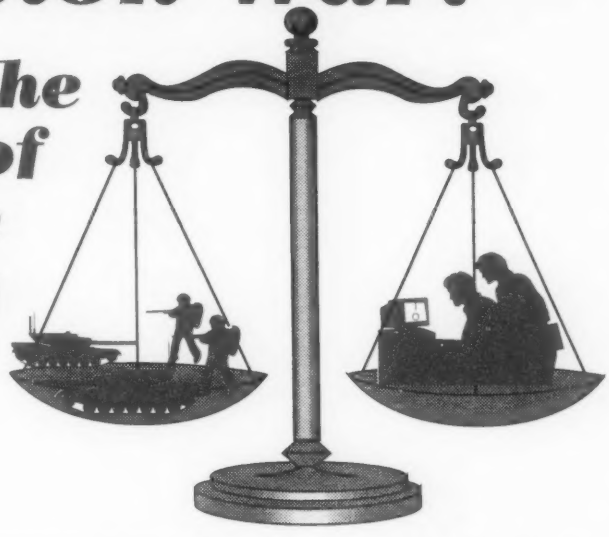
Conclusion

Battlefield visualization shows great potential for the future. XVIII Airborne Corps' aggressive prototyping effort has enabled a running start for the fiscal year 1997 RBV ACTD and rapid integration of two BV prototypes within the EXFOR. The BV system will provide commanders the ability to see their physical battlefield and the disposition of friendly and enemy forces arrayed on it in a high-fidelity, virtual environment, and to plan, wargame, and rehearse an operation before ever making contact with an adversary. This capability will give the Force XXI commander a significant advantage over any opponent, and provide the critical enabling technology to gain information dominance at critical times on the battlefield.

Captain Jones is currently the Operations Officer in the Office of the U.S. Army Deputy Chief of Staff for Intelligence (DCSINT) Initiatives Group. He has a bachelor of arts degree in Public Relations from the University of Georgia and a master of science degree in Personnel Management from Chapman College. Readers who wish more information may contact the DCSINT Initiatives Group via E-mail odcsint@access.digex.net and at (703) 695-2968 or DSN 225-2968.

Information War:

Rethinking the Application of Power in the 21st Century



by Douglas H. Dearth

The views expressed in this article are those of the author and do not reflect the official policy or position of the Defense Intelligence Agency, Department of Defense, or the U.S. Government.

Among First-World powers, there has emerged in recent years a form of "Third-Wave War" to match the evolution of "Third-Wave Societies." The hallmark of both is information. The Tofflers' book, **War and Anti-War: Survival at the Dawn of the 21st Century**, is a paean to the work of the U.S. military over the past twenty years to essentially "reinvent" itself in these terms.[1] The evidence and effectiveness of this fundamental change was evident to an extent during Operation DESERT STORM in 1991.

A Conflict of Decision Processes

Just as information is changing society, it is also changing concepts of national security, the definitions and parameters of battlespace, and the measurements of force. "Force" is becoming less tangible and more dependent upon qualitative factors. Battlespace is expanding greatly in terms of frontage, depth, and altitude. Movement rates—for forces, materiel, and ideas—are increasing; therefore, time is shrinking. War is becoming more a conflict of decision processes, and success will be determined by the "information differential" between forces and between commanders. "Third-Wave War" is "Information War." These "post-industrial war" operations must be not only "joint" and "unified," but "holistic" and "simultaneous."[2]

What Is Information Warfare? Tom Rona, the probable originator of the term, essentially would describe information warfare (IW) as a *"battle of decision systems."*[3] While something of a groundbreaking concept, especially in the 1970s, this is essentially a technical approach; from some perspectives, warfare has always been a struggle between decision systems. Professor George Stein of the Air University holds that the concept is broader. He said *"Information warfare, in its broader sense, is simply the use of information to achieve our national objectives."* Further, he says that *"Information warfare, in its essence, is about...the way humans think and, more important, the way humans make decisions."*[4]

The Tofflers would describe IW in broader terms: as *"a new 'warform."*[5] Their concept is that **IW is a way of thinking about war, warfare, and conflict. It is a different way of applying military power.**

In fact, part of the mystique and promise of IW is that it may be broadly applied as part of a national policy designed to obviate the need for traditional military involvement. In some ways, it is political war beyond the bounds of diplomacy in which weapons are intangible in appearance and very tangible in result. This is a new breed of weapon which leaves neither a "smoking gun" nor plausible trace. It is a weapon—and a campaign—which a head of state may launche with or without the involvement of his military force options.

IW also constitutes an operating or conflict environment. The attempt to "digitize the battlefield" currently under way in the U.S. Army, on its face seems to be a limited technical approach to the broader issue. It is not inappropriate; in fact, it is necessary, and tacitly acknowledges that something is significantly different in the arena of armed conflict. Others would describe IW as simply "command and control warfare (C^2W) by another name." It is not. C^2W is the tactical applica-

tion of the much broader phenomenon of IW.

The Department of Defense defines IW as—

...actions taken to achieve information superiority by affecting adversary information, Information-based processes, information systems and computer-based networks, while defending one's own information, information-based processes, information systems, and computer-based networks.[6]

The current confusion about these concepts is further exacerbated by the introduction of other new terms like "cyberwar," "netwar," and "knowledge war."[7] All of these concepts are valid. It is inescapable that **there is something qualitatively different about warfare in the information age.**

Characteristics of Information War

Continuous, Simultaneous, Accelerated, and Non-linear. At the heart of the IW concept is the idea of achieving military objectives with an absolute minimum of force application and cost. Although this has always been a warfighting objective, in the past the ability to achieve this objective depended upon a number of variables, many of which the potential or real enemy controlled.

With the information revolution, however, the minimum force or cost objective becomes attainable by the side that has **information dominance.** If we have continuous, real-time surveillance of a potential adversary's military forces, we can simultaneously position our forces to achieve and maintain an advantage. We may deter or preclude adversary use of military force altogether by communicating this advantage and our intentions, perhaps with additional information like psychological operations and deception routed through other channels to further complicate his decision process. Even failing that, by maintaining more perfect knowledge of enemy force disposition and positioning our forces accordingly while denying the enemy knowledge of our disposition, we can maximize the effectiveness of any force application, thus allowing use of only as much force as is necessary to achieve our objectives. In addition to maintaining the element of surprise, because we immediately know the results of our application of force on the enemy, we can accelerate our response to changes in enemy activity and tailor our re-application of force to only those critical nodes that require it.

By dominating the adversary's information systems, along with the use of smart stand-off weapons, we will be able to impose our will on the enemy without the costs associated with occupying his territory. Rather than moving through a battlefield in a linear fashion, we will continuously be able to select and neutralize critical targets in a non-linear battlespace "just in time," thus obviating the need for a large inventory of backup weaponry.

Instant Feedback. The ability to take the right action just in time depends, of course, on feedback. Since the beginning of human organization, decisionmakers have sought information about the results of their decisions as soon as possible, so that if corrective or reinforcing actions were required, they could be taken while it was still possible to influence the course of events set in motion by the initial decision. Until relatively recently in our history, the ability to gain such information was limited by many factors, but most especially by distance.

Electronic communication will change all this, particularly the advent of communications satellites and high-capacity fiber-optic cables. Decisionmakers can now remain "plugged in," not only receiving instant feedback on the effects of their decisions, but also using these same lines of communication to transmit new decisions based on the feedback information.

The concept of instant feedback as it relates to IW is viewed in the context of a closed system, whether the F-117 or the Army's "digitized battlefield" envisioned in Force XXI. Instant feedback, or something close to it, applies at all levels of decisionmaking. While the media may not be responsible for the United States "losing" the war in Vietnam, public reaction to the combat images brought into our homes most assuredly influenced the decisions made by the Johnson and Nixon Administrations on prosecution of the war. During the Gulf War in a speech covered live by the Cable News Network (CNN), Saddam Hussein called for a debate with President Bush; within thirty minutes, President Bush held a press conference to advise the world (and Saddam) that he had no intention of participating in such a debate. Even in non-democratic societies, both leadership and the general public are simultaneously aware of the results of policy decisions via television news coverage.

The point here is that, as Professor Stein noted—

the worldwide infosphere of television and broadcast news...[will] shape the political context of the conflict. It will define the new "battlespace." We face an "integrated battlefield," not in the usual sense of having a global positioning system (GPS) receiver in every tank or cockpit, but in the Clausewitzian sense that war is being integrated into the political almost simultaneously with the battle.[8]

Under such conditions, the distinctions between the tactical, operational, and strategic tend to blur into insignificance. Like it or not, the actions of a single soldier, caught by the international media, can potentially affect the outcome of a conflict.

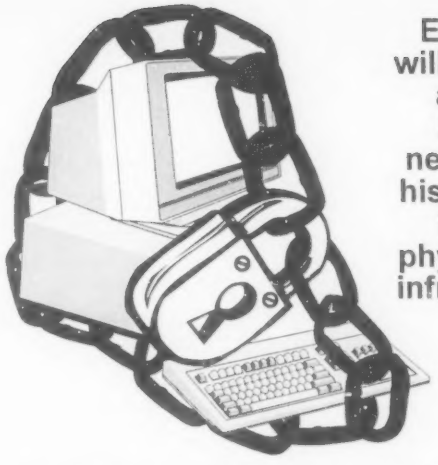
The problem with this, Stein points out, is that this media-created world is a "fictive universe," not because the images are un-

true, but because they do not contain sufficient information to capture the context and totality of the truth. The average "sound bite" (actually a "video bite") on the news is somewhere between 8 and 12 seconds—very little time to articulate a policy position. In a perfect world, decisionmakers would have perfect instant feedback on which to base subsequent policy decisions. In the real world, the temptation to rely on timely fictive feedback, as opposed to less timely but more fulsome feedback from intelligence or other official sources, may prove to be overwhelming.

Blurred Levels of War. Information technology is increasingly blurring the levels of war. Efforts at the tactical level of war—at which engagements and battles are fought for limited objectives—are aggregated at the operational level of war in the form of campaigns. This process musters broader efforts over wider terrain and space and time in a theater of operations. These in turn are directed toward the achievement of national war goals at the strategic level in theaters of war. These three levels of war historically have been distinguished by the size of forces and volume of resources employed, the breadth of terrain and space over which forces deploy, and the time expended in the prosecution of operations. There has been a realization, too, that these levels overlap somewhat.

Since at least the Napoleonic Era, the distinct military trends have been toward larger and more varied kinds of forces employed over increasingly broader terrain, space and distance, often with the decision cycles of operations consuming decreasing periods of time. Various aspects of information technology and IW provide the prospects for significant change in certain of these trends:

- ☐ Mechanisms of force continue to proliferate, but the size of forces can decrease.



Electronic combat will potentially enable a commander to inflict "effective neutralization" upon his opponent without the necessity of physically destroying infrastructure, forces, or people.

- ☐ Breadth of terrain and space and distance can continue to grow to the physical limits of the planet and into space.
- ☐ Time will continue to shrink with the increase in the speed with which and distance over which we can employ force.

Hence, the discernible distinctions among the levels of war will be increasingly blurred; this will complicate the nature of political and military planning and decisionmaking.

The "packaging" of IW into a division of labor that fits convenient military doctrine and organization may be passé. The smallest team of specialists, operating covertly under direct civilian control and tasking, could apply strategic, operational, or tactical IW tools against any level of an adversary's decision system. Military knowledge and supervision need not necessarily be a consideration in the planning, but may be significantly influenced by the results.

Blurred Civil-Military Divisions. In a similar fashion and for the same reasons, the Uptonian distinctions between the civilian and military realms[9] are being blurred. The Clauswitzian concept of the trinity of "Army" (really "Armed Forces"), the "State," and the "People" is more valid than ever on one level: in the information age, the state and armed forces will no longer necessarily possess a monopoly over the means of violence—especially "information violence." Further, national centers of gravity increasingly will reside in the civil sector. These centers of gravity include the national banking and finance industries and power generation and distribution systems. The civil sector, in terms of production and morale, has long been important to warfare. However, in an age when production is measured more in terms of intangible knowledge than tangible goods and the value of knowledge applies equally in both the civil and military sectors, the distinction between the two realms will blur even more. Further implications are that in the future civilian infrastructure will be an even more prominent target of attack than was the case in the industrial era, but it cannot be defended by military forces.

War as Work: Third-Wave War. The basic characteristics of the new "war-form" essentially mirror those in the civilian economy. As the Tofflers observed, nations make war the way they make wealth. The watch-words are **information dominance** and **information assurance**.

- ☐ Knowledge becomes the core of military power and the central resource of destructivity, rather that pure brute force, and "intangible values" more accurately determine the mili-

tary balance, rather than hardware.

- ☐ Decreasing the massing of forces requires increased precision and more selectivity in the application of military power.
- ☐ Military "work" is more often dependent upon education and expertise than traditional machismo and brute force; information will become the nature of war. Innovation is increasingly prized; improvisation replaces rote and routine.
- ☐ Organization becomes more fluid and less hierarchical. Integration of all assets, forces, and services is essential.
- ☐ "Acceleration" characterizes operations at all levels (not necessarily absolute speed, but speed relative to the enemy's pace of decisionmaking and movement—his *"OODA-loop"*).[10]

These characteristics of IW will affect combat arms, as well as combat service and combat service support functions, most markedly in terms of intelligence, signals, transportation and logistics.

War as Improvisational Theater.[11] In the future, we will be operating in a very media-rich environment, where our military actions will be broadcast instantaneously via worldwide television. Think of the intelligence and operational security implications of private-sector news media operating their own remote-sensing imaging satellites, which certainly will happen within the decade. Consequently, military commanders must be increasingly adept at operating effectively in this environment. If we consider a military operations plan (OPLAN) a script, the ensuing events will increasingly resemble improvisational theater on a global stage where reactions of a variety of audiences and critics can ultimately determine the difference between success and failure in a political, if not military, sense.

At Mogadishu, Somalia, SEALs reconnoitering the beach in the glare of the lights of the assembled video cameras looked more silly than formidable. It was an inauspicious beginning to what was to become a well-intentioned but ultimately frustrating and futile military exercise.[12] Consider also the image of illiterate thugs on the docks of Port-au-Prince, Haiti, who greeted U.S. and Canadian troops aboard the USS Harlan County, waving their English-language placards and shouting (for CNN's cameras) that Haiti would be "another Somalia for America." We then watched as the Harlan County steamed away, much to the consternation of the U.S. military advance party waiting on the wharf. When the U.S. advance elements of the North Atlantic Treaty Organization's Implementation Force (IFOR) entered Tuzla, Bosnia, they found themselves outnumbered by the media at easily a ten-to-one ratio. Because the global information infrastructure is nothing if not interactive, commanders may find their OPLANs or "scripts" being rewritten as they go along. The level of "script" adaptability may be a critical predictor of success for military operations in the information age.[13]

Implications of Information Warfare

The United States and other Third-Wave societies are undergoing changes in both the ends and means (but not the purpose) of war. Despite these changes, it is highly unlikely that armed conflict will totally disappear into cyberspace.

Proliferation of the Means of Conflict. The rigorous application of information technology to warfare means, first of all, that there will be a proliferation of the ***means*** of conflict. To the traditional means of firepower and maneuver will be added the means of attacking one's enemy ever more powerfully **electronically**. One can not only attack his command and control (C^2) systems with destructive firepower, but with other destructive technological means. Disinformation, rumor, and propaganda have long been means of attack and these means are now enhanced. Some have speculated that effective deception operations are no longer possible in the age of satellite reconnaissance. The effectiveness of deception depends upon available "channels" of information and the penchant of one's opponent for self-deception. Hence, the possibilities for successful deception operations have never been better.

Lethality versus Effectiveness. Electronic combat will potentially enable a commander to inflict "effective neutralization" upon his opponent without the necessity of physically destroying infrastructure, forces, or people. Military professionals often overlook the fact that the purpose of warfare is not "killing people and breaking things." Those have been the **mechanics** of war, not its **purpose**. The purpose of war is to inflict your **will** upon your opponent. If one's will can be imposed—modifying the opponent's behavior or intent—without widespread physical destruction, the post-conflict possibilities for political reconciliation and human progress may actually be enhanced. War in the information age holds out at least the prospect of that eventuality.

If this has validity, we now have the prospects of fundamentally changing the way we conduct war and the desired ends. The traditional ends of war were to destroy the opponents's forces in the field, in the air, and on the seas; to destroy his productive war capacity; to subdue his population; and to occupy his capital. With the destruction or disabling of his C^2 capability and the ability to control the perceptions of his policy elites and population, there is the possibility of working one's will upon the opponent without necessarily wreaking physical havoc upon the infrastructure and population of the enemy. The cal-

culation can be humanitarian or purely utilitarian in terms of preserving the economic wherewithal to sustain a viable and productive society with altered political aims.

Clausewitz and Anti-Clausewitz. Much of this analysis flies in the face of traditional Industrial-age warfare. In the military forces, there is an ingrained "Clausewitzian" value system, and we have been raised within it. Much of the foregoing discussion contradicts the Clausewitzian approach to warfare as taught in our staff and war colleges. Clausewitz still has much to contribute to military thinking, even in democratic societies. The trinity of state, armed forces, and people is crucial, and its continued importance cannot be over-emphasized, although his emphasis on physical destruction and annihilation may be outdated. The possibility of the decisive winning battle (at least in peer-competitor warfare) could theoretically be resurrected. The danger for "Third-Wave" societies is that the potential for success in this regard may well rest with niche-competitors in asymmetrical conflict.

Time, Distance, and Speed. Since the early days of the industrial age, time compression has increased, yet time has become more important. Clocks for centuries had only hour hands; today, many endeavors measure time in hundredths of seconds. Initially, transportation technology drove this compression. There followed the telephone and the facsimile machine, then television, which introduced the added dimension of more vivid graphical images. More recently, it has been the computer—particularly the microprocessor—linked via local- and wide-area networks. Thus, speed has increased ever more dramatically as a function of distance. The result is that **distance means less—and, hence, time is compressed.**

The instant feedback provided by modern electronic communications affects the political, cultural and social spheres as readily as it does the commercial and military arenas. Recall President Bush's near-real-time response to Saddam's challenge to a debate on global television in 1990. By the same token, cultural and social trends proliferate very quickly among the Third-Wave countries and to the rest of the world. The global currency market now operates 24 hours a day, and the stock and commodity positions are calculated instantaneously. The U.S. Air Force's Air Tasking Order procedure now demands a 24-hour turn-around against military targets.

Expectations. The result is not just efficiency—the saving of time and labor. It is that, but it is far more. It changes peoples' expectations. They understand that they **can** know more about more things with a lower expenditure of effort and faster; this understanding turns to a **want** and then **demand** to know more, faster. People's expectations also have changed by virtue of **what** they know. Reading about events is different from viewing vastly more life-like images on a screen. It is much more realistic, because interpretation is easier. It requires less imagination, and at the same time it fires the imagination. While people are drawn to the vividness of the images, they can be repulsed by those same images. The interpretation is more intense. Politically, the potent images of starving Somali children, butchered Rwandans, or a bludgeoned Los Angeles motorist virtually demand a prompt political response. Generations of computer technology will progress in 18 to 24 months, rendering corporate and government management and procurement policies laughable.

For the military, and government generally, the omnipresent and seemingly omniscient global media mean that every decision and action is immediately transparent to national and international scrutiny. For now, even a single military casualty will be the subject of immediate coverage and public scrutiny. The risks will be hyper-sensitive decisionmaking and timid military leadership in the face of fickle public emotions.

Erosion of State Sovereignty. Increasingly, the traditional attributes of the nation-state are eroding, and much of this erosion results from the influence of information technology. In the age of information violence, the state will not be able to dominate the means of force, nor will the state necessarily be able to deter or defend against information attack. States also are no longer the only—or necessarily the most important—actors in the international arena. Increasingly, the non-state actors deal across state boundaries with each other and with states on a nearly independent footing. There is a general erosion of the concept of sovereignty. While some of the nation-states are "failing" because they cannot fulfill the basic traditional criteria of sovereignty, mature and successful states also are witnessing a similar erosion of traditional controls, largely as a result of the effects of information technology. The state will not fade away. States will remain as primary and important actors in the international arena, but they will represent only one of many forms of political organization, power, and interaction.[14]

The purpose of war will not change from that of imposing one's will on one's opponents. The nature of war, however, will change considerably

Global Information. National control of information is tenuous—if it is possible at all. The same is true for IW. Moreover, the global information infrastructure is becoming more ubiquitous every day. With the multiplicity of media, access, and service-providers comes a redundancy and surviv-

ability that challenges the notion of denial and disruption of service. The threshold of the information age saw the successful severing of Panamanian and later Iraqi command, control and communications and telecommunications, but the world has learned from these experiences. Aiding the learning process has been a steady erosion in the acquisition and operating costs of digital communications. Whether the threat is fire, flood, or IW, systems developers continually add new tools to their capabilities for assuring service via alternate routes and standby systems.

Public Diplomacy. "Public diplomacy" is a term that refers generally to those government activities designed to inform and influence foreign publics. If traditional diplomacy is state to state, public diplomacy is from state to the foreign populace. Although not a new concept, it has taken on new importance over the past decade as a result of the global communication explosion. Moving beyond the traditional, usually defensive, concept of the Public Information Office, the U.S. military has developed mechanisms like the Military Information Support Team in Haiti and the Combined Joint IFOR Information Task Force in Bosnia. The intent of both is to aggressively pursue the public information quotient in support of military operations.

Conflict in the Information Age

War, Conflict, and Force. All war and conflict will not change, but in many cases it will. **The purpose of war will not change** from that of imposing one's will on one's opponents. **The nature of war, however, will change considerably.** In forces configured for IW, the preference will be conflict dominated by the advanced nature of decision systems and by more subtle means of waging war. These forces configured for IW will have at their disposal a wider array of the means of destruction, but the nature of those mechanisms will result in proliferating the means of conflict. The traditional means of firepower and maneuver will be augmented---and perhaps in the long run replaced---by methods of attacking one's opponents with electronic technological methods. The ultimate outcome of applying those methods, however, will not necessarily be free of lethal outcomes.[14]

It is a common conceit of advanced nations and their armed forces that they can impose their wills on the lesser powers and relatively primitive forces through application of advanced technological means. Painful historical experience since the late 19th century indicates just the opposite. "Low-intensity" conflict (or the current concept of "operations other than war") is not a "lesser case" of higher-order strategy and doctrine and the tactics, techniques, and procedures that support them. Relatively primitive forces will---and do---have access to sophisticated technology, and they will know how to use it. Advanced technology will be increasingly available. While such relatively sophisticated concepts as "air-battle management," "air-land operations," and "dominating maneuver" might be lost on them, there will be some opponents who do understand "perception management" and "information warfare" in its rudimentary sense.

Another conundrum will face sophisticated military forces: the possible passage of what might be called "heroic warfare." If the Tofflers are approximately correct that a hallmark of future combat is "brains over brawn," a change will be required in the selection, retention, development, and promotion of "cyber-warriors" who attack the enemy and defend the nation by means other than cold steel and hot lead. This possibility might appeal more to a nation that shies from incurring combat casualties; it likely will appeal less to their military subcultures that intrinsically value blood sport, distance running, and the machismo self-image.

The Social Impact of Information War. It is difficult for democratic society to discern "good news" from the prospects of war. If there is any good news to infer from the kind of warfare likely to predominate in the 21st century, it might be the prospects for reduced levels of physical and human destruction. Among Third-Wave peer-competitors, at least, perhaps humankind will be spared the tens of millions of civil-

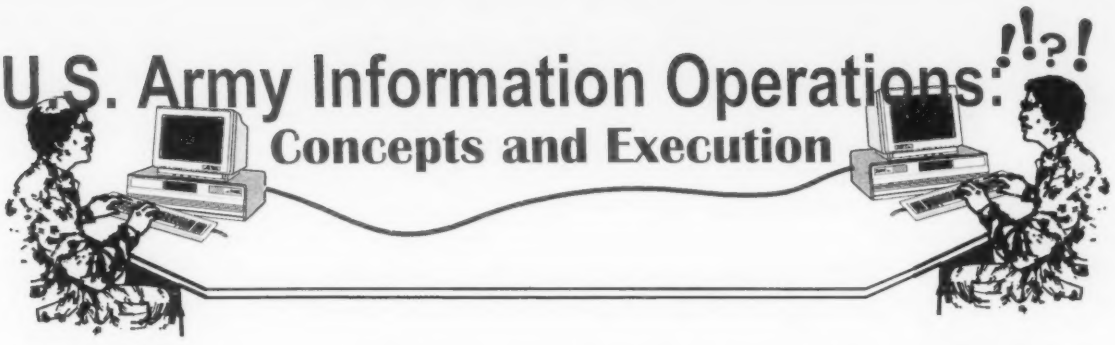
(Continued on page 60)

Combat Developments Goes On-Line

The Directorate of Combat Developments (DCD) at the U.S. Army Intelligence Center and Fort Huachuca has a new home on the World Wide Web. The intent of the new DCD Homepage is to be a forum for information exchange with the field, as well as a tool for the electronic staffing and sharing of documents and publications. The page currently includes information such as the mission and organization of DCD, POC listing and an E-mail directory capability to individual DCD addresses from the Web. DCD intends to include information about new concepts and architectures, intelligence and electronic warfare systems, force design issues, and links to other intelligence pages.

The page has been optimized to work best with Netscape Navigator 2.0 but other graphical browsers will also work. The DCD Homepage URL is http://huachuca-dcd.army.mil. Look for additional features, such as hyperlink capability to DCD's Battle Book to come on-line in the future. For more information or answers to questions you may have, contact Captain Brent Horrocks at (520) 533-1837/2010, DSN 821-1837 or via E-mail at horrocksb@huachuca-emh1.army.mil

U.S. Army Information Operations: Concepts and Execution



by Captain James E. McConville, USAR

The 21st century is not waiting for the Army; it is already upon us; and we must meet its challenges three ways. First, we must understand the information age battlefield. Second, we must modernize to take full advantage of information age technology. Finally, we must continue to develop the programs that "enable" the power projection strategy.

—General Gordon R. Sullivan, Former Chief of Staff, U.S. Army[1]

The United States Army faces the requirement to move into a new age. The coming of the information age has given us an unparalleled opportunity to improve the efficiency and effectiveness of our ground forces. What is needed is the vision and the will to design, field, train, and use the force of the 21st century.

It cannot be denied that a massive change is under way in our society, a change driven by the advent of advanced information technology. New information collection, analysis, communication, and display capabilities have changed the way we think, act, and organize, whether in industry, education, or in the military. Driven by the irresistible force of the emerging capabilities, and steered by some visionary military leaders, the U.S. military has become the preeminent force in the world of military technology.

The realities of the information age promise to alter forever the way the military does business. In addition to precision weaponry, the Army sees its future in the advanced collection, processing, analysis, communication, and display of massive amounts of information. The information age promises to reduce Clauswitz's daunted *"fog of war."*[2] The employment of precision weapons, precisely targeted, teamed with maneuver decisions incorporating clear battlespace visualization, while simultaneously defeating the adversary's visualization of the battlefield, will ensure that our force remains the dominant military force deep into the 21st century.

Definitions and Doctrine

One of the driving technological changes behind the development of IO is the expected revolution in our ability to move, process, analyze, and present vast amounts of information to decisionmakers quickly, and understandably. To maximize the impact of the increased information capabilities now available, the Army must learn to fight on the information battlefield. To this end, the Training and Doctrine Command (TRADOC), the Army's concept and doctrine development arm, has published **FM 100-6, Information Operations**, dated 17 August 1996. This manual establishes the guiding principles for the use of information on the Army battlefield. In order to further refine the concepts described in **FM 100-6**, the U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH) created the IO Task Force and conducted an IO wargame in November 1995. The wargame, which included participants from more than 27 agencies and units from all over the DoD, clarified and refined the application of IO to the Army battlefield. This article presents some definitions and then summarizes the findings of that wargame in terms of IO requirements and integrating IO into the force.

What Are Army Information Operations? FM 100-6 describes IO as—

Continuous military operations within the military information environment that enable, enhance, and protect the commander's decision cycle and mission execution to achieve an information advantage across the full range of military operations. Information operations include interacting with the Global Information Environment and exploiting or denying an adversary's information and decision systems.

This definition is successful at capturing the major elements of Army IO:

- ☐ IO are continuous. They are conducted during peacetime and war.
- ☐ Army IO involves interacting within the global information environment (GIE), while operating within the military information environment (MIE). (See Figure 1.) This describes the requirement to maximize the use of all information available in order to assist the military commander to achieve operational success—information from military systems and open sources like the media, the Internet, and other global access information systems.
- ☐ Army IO focuses on the decision cycle, supporting more informed decisionmaking by the friendly commander, while denying the enemy decisionmaker full use of his decision

cycle through the IO attack element.

- ☐ The goal of Army IO is the achievement of an information advantage (dominance) over the adversary. This advantage is for better mission execution, it is not the goal in itself.

Why IO, Not Information Warfare? Army IO doctrine reflects, and goes beyond, the joint military strategy of command and control warfare (C^2W), which implements DoD IW policy. Recognizing that IW as currently defined by DoD is more narrowly focused on the impact of information on actual conflict, the Army has chosen to take a somewhat broader approach to the impact of information on ground operations and adopted the term "information operations." The Army chose this broader approach for two primary reasons. First, it recognizes that information issues permeate the full range of operations from peace through global war. Second, this broader approach emphasizes the operational impact of information on knowledge-based operations at each and every echelon.[3]

Editor's Note: In Fall 1996, there was discussion among the Services and the joint staff about adopting the term "information operations" but keeping the same meaning used for "information warfare."

The Components of Army IO. Doctrine describes IO as having three parts: intelligence and other relevant information, information systems, and command and control warfare (C^2W). In general terms, IO comprises the information required, the systems needed to move and use that information, and the ability to manipulate the information (attack and protect) in order to gain a C^2 advantage.

- ☐ Information. Information is the currency of IO, the data that, once controlled and understood, leads to information dominance and the tactical advantage on the battlefield. **FM 100-6** defines information as *"data collected from the environment and processed into usable form."* Military information includes intelligence (the processed and analyzed information on an adversary), friendly force information, and environmental information (terrain and weather). Together they become battlespace visualization.
- ☐ Information Systems. Unless information reaches the decisionmaker in a timely manner and understandable form, it will not contribute to success on the battlefield. The information system must be secure at multiple classification levels, provide seamless access to databases at national through tactical echelons, and versatile enough to adapt to the many force configurations found in today's Army. It must also be simple enough to allow full integration into the force.
- ☐ C^2W. Army IO does not neglect the attack and protect aspects most commonly associated with IW. C^2W is—

...the integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary capabilities against such actions. C^2W applies across the operational continuum and all levels of conflict.[4]

Military commanders use C^2W to manipulate the information environment and achieve a tactical advantage. *"C^2W provides the 'sword' against an adversary's C^2 system, and the 'shield' against the counter C^2 actions of the adversary."*[5]

The Endstate: Information Dominance. As was stated above, the goal of IO is to create an information advantage—information dominance. It is a delta:

...the difference between the aggregate of information available to each of two opposing military commanders. But it is more than just information: it is the difference in understanding of information in the context of some specific purpose that is the crux of the definition."[6]

The delta sought is seen in terms of battlefield visualization.

What is the "value added" of IO? What does this new concept contribute to the mission and objectives of the tactical commander? Based on the outcome of the IO Wargame held by USAIC&FH in November of 1995,

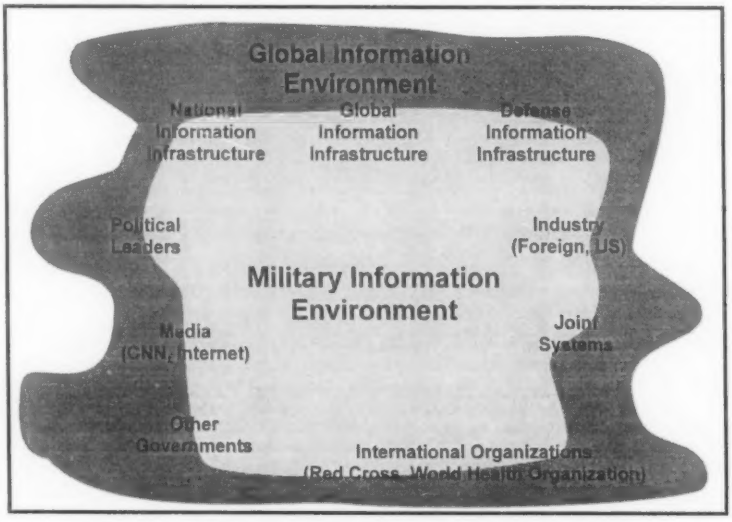


Figure 1. Information Environments (GIE and MIE).

the value added of IO and C^2W is the **massing of information effects.** C^2W, when teamed with the other parts of IO, can deliver information dominance at the specific place and time when the commander wants or needs it. C^2W does not act alone to create information dominance, but it does provide the power to determine when that desired state will be achieved.

Requirements for Information Operations

The IO Wargame was a force-on-force, U.S. Army corps-level simulation using information effects on the tactical battlefield. The wargame clarifed several types of requirements for tactical IO. These include intelligence, battle command, C^2W, and information systems requirements (see figure 2). These findings point clearly where the Army must go to integrate IO into the force and make tactical IO a reality.

Intelligence Requirements. One of the most common observations made by wargame participants ("players") was that the intelligence system and the intelligence community have a very tall order to fill to achieve the goal of tactical IO. The consensus was that not only would we need to deliver intelligence faster and farther than ever before, but that the nature of the intelligence will change, both in focus and specificity.

The essence of C^2W is its focus on the decisionmaking processes of both the friendly and enemy commander. Each C^2 mission, whether C^2 attack or C^2 protect, has as its ultimate objective a decision. While this played out well in the wargame, it was clear to all players that this "decision war" requires we know much more about how and why adversary tactical military commanders make decisions. In the context of the wargame scenario we used it was clear that this data does not exist, especially in a form available to corps-level planners. Some of the questions for which C^2W planners need answers cover adversary----

- ☐ Intelligence organization and capabilities.
- ☐ Information systems and communications equipment and networks.
- ☐ Military decisionmakers, their decision criteria, and outside influences which may effect their responses.

To achieve tactical IO, we need comprehensive information about adversary command, control, communication, computers, and intelligence (C^4I) capabilities. We will need to know the points of failure in enemy communications systems, how to target them, and where and when they are most vulnerable. Additionally, much information is needed on the technical characteristics of enemy intelligence collection equipment, including signals intercept, imagery systems, visual systems, target acquisition systems, and the like.

Delivering the intelligence needed for C^2W and all other military operations and for achieving information dominance, presents a unique set of requirements to the intelligence system. It is here that the emerging tactical intelligence system shows the vision of intelligence planners from recent years. The realization of their vision is a system of systems driven by commander requirements, synchronized with operations, seamless between national and tactical levels, and supporting a force projection Army, that will satisfy the demands of IO.

Massing information effects means intelligence planners must have the right information, at the right place and time. The challenge is to collect the intelligence desired by the commander, as expressed in his intelligence requirements, with the correct lead-time to deliver it to him when and where he needs it.

Battle Command Requirements. Information operations, the intelligence that supports them, and the information systems on which they rely, need commanders who are able to visualize the battle more accurately and, based on that visualization, relay to planners the endstate of the operation that they desire. This visualization of the battlespace is in itself an information operation. To reach it, several capabilities are required, including----

- ☐ A dynamic common picture. Commanders need a system that visually displays the situation in an easily understandable format, based on the most up-to-date intelligence, environmental, and friendly force information available. (When the information changes, the picture must change as well, thus the term "dynamic.")
- ☐ Improved statement of the commander's critical and priority information requirements (CCIR and PIR). Determination of the CCIR and PIR is a key part of mission planning.
- ☐ Automated decision support and battlefield operating system (BOS) synchronization. One of the most difficult tasks faced by the IO-C^2W planners during the wargame was the synchronization of the C^2W elements, the information requirements, and the information system requirements with the overall tactical plan. With so many operations being executed at so many levels, it is extremely difficult to determine when to create the "massed information effects" the planners are after. A large part of that difficulty is the inability, using existing tools, for planners across the BOS to share planning data and link together activities and decisions that will occur in the battle plan. Like the staffs trying to portray the common picture, these planners need an automated, dynamic, and flexible tool to tie all these distinct, yet interoperating, activities together. Like the automated intelligence and electronic

warfare (IEW) synchronization matrix, this tool must link planners both horizontally and vertically.

- A mission rehearsal tool. Battlefield visualization requires not only a dynamic and accurate picture of the current battlefield, but also the ability to assess the possible future situations in an accurate and reliable manner. Tied to the IEW synchronization effort, the common picture, and automated BOS synchronization is the mission rehearsal tool. This will allow commanders and staffs to model the results of their plan prior to execution. This advanced simulation must build its scenario from the dynamic common picture, and will, when complete, be able to adjust the model's outcomes based on changing inputs from the real intelligence and operational information received.
- The ability to think in terms of Information dominance. All of the technology and staff processes will come to nothing if we are not successful at teaching our military commanders and staffs to think in terms of information dominance. To aid commanders in describing the endstate of their information operations, we must teach and train them and their staffs to do this.

C^2W Requirements. C^2W is the IW application of IO. It delivers information dominance to the commander through the manipulation of the information battlespace, either by protecting one's own information or attacking the adversary's. C^2W is the synchronized and integrated use of OPSEC, EW, deception, PSYOP, and physical destruction to achieve information dominance.

As our wargame proved, the most important factor in C^2W is synchronization. It is by synchronizing all the elements with the overall battle plan, that C^2W is able to mass information effects and contribute to tactical information dominance. To do this, the C^2W plan must be an integral part of the entire mission planning cycle.

Full staff integration allows C^2W planners to develop their operational objectives and goals based on visualization of C^2W and C^4I capabilities and vulnerabilities. Incorporating the commander's intent and visualization of the endstate and the activities of the other BOSs, the C^2W planner can develop his course of action. To do this efficiently, he must determine where, when, and how to attack the adversary's decision cycle, and where, when, and from what to protect his own. To this end, any battlefield visualization tool must include the capability to graphically depict the friendly C^4I architecture, and overlay it with the adversary C^2W capability. Like the common picture, this graphic must be automatically updated, dynamic, and tied to the mission rehearsal toot for IEW and BOS synchronization.

To conduct sophisticated C^2W, we must be able to leverage the capabilities of national information warfare against targets that support the objectives of tactical commanders. Concurrently, targets attacked at the tactical level can seriously impact the conduct of national information warfare. It is crucial that C^2W and IW planners have the ability to communicate and coordinate C^2 attack requirements among echelons, respond to those requirements in near-real time, and to deconflict missions among the various C^2W and IW agencies. The Land Information Warfare Activity (LIWA) is preparing to take on this responsibility.

Information Systems Requirements. The ability to realize the linked, timely, well-presented, secure, flexible, and worldwide accessible communication and data transmission systems is key to the achievement of the information operations vision of Force XXI. The basic requirements for the system are—

- Global connectivity, seamless between echelons, that is deployable and adaptable to different force packages and areas of the world.
- Secure and redundant systems that can be continuously checked for intrusion, re-initiated, and cleared if intrusion occurs.
- Multifunction access to a common system, scaleable and adaptable according to the user needs. The system must be shared by intelligence, maneuver, fire support, communications, and other battlefield functions, yet be able to display the only information requested by the user.
- Advanced display capability that contributes to the common picture. Incoming data must feed directly into the fusion, processing, and analysis tools used by the various planners, and assist in the presentation of the common picture to the commander.
- Access to GIE information systems. The system should allow for interconnectivity and access to non-military open source systems when that access is desired by the commander or user.

Integration of Information Operations into the Force

Smart commanders have always done IO. Our task now is to ensure that all commanders, staffs, and soldiers think, act, and operate to achieve information dominance. The wargame participants discovered some insights on how best to do this.

Concepts. Two major conceptual adjustments needed to be made in order to fulfill the vision of tactical IO. First, while the doctrine exists for the establishment of the CCIR and PIR, it needs more emphasis. Commanders must understand that unless they clearly establish their information requirements, based on endstate

of the battle as they visualize it, they will never be able to take full advantage of IO. Second, staffs and commanders must begin to view the battlefield in terms of decisions—friendly and enemy. The Army must plan operations to support the needs and requirements of those decisions just as it plans to destroy and protect combat power.

Doctrine. In general terms, the problems experienced by many Army professionals is understanding that IO can be solved by bounding the problem in terms of information dominance. This end-state makes it clear to all where we are going with the IO concept, and provides focus by giving planners and commanders an objective for which to strive.

In the future, "separate" IO doctrine could be unnecessary as IO becomes an integral part of the way we all think about military operations. However, most wargame participants agreed that C^2W needs a separate "how to" manual to show staffs how they should integrate the more aggressive part of IO into their battle plans. The manual would include tactics, techniques and procedures for accomplishing C^2W.

Organization. The Army corps needs a full time C^2W officer. This officer is responsible for bringing the perspective of information dominance into the established corps planning structure (G3 Plans and the Deep Operations Coordination Cell). The C^2W officer is responsible for synchronizing the capabilities of the C^2W elements, leveraging the capabilities of higher echelon IW agencies and units providing connectivity with national- and theater-level IW agencies, and monitoring the execution of the elements of the C^2W plan, to ensure the delivery of massed information effects when needed.

During the IO Wargame, the need to develop a C^2W cell in the corps analysis and control element became apparent. Due to the specific and unique requirements of decision modeling, threat IEW synchronization, and the like, it is imperative that a dedicated set of specifically trained analysts assist the G2 in preparing the information needed by C^2 planners.

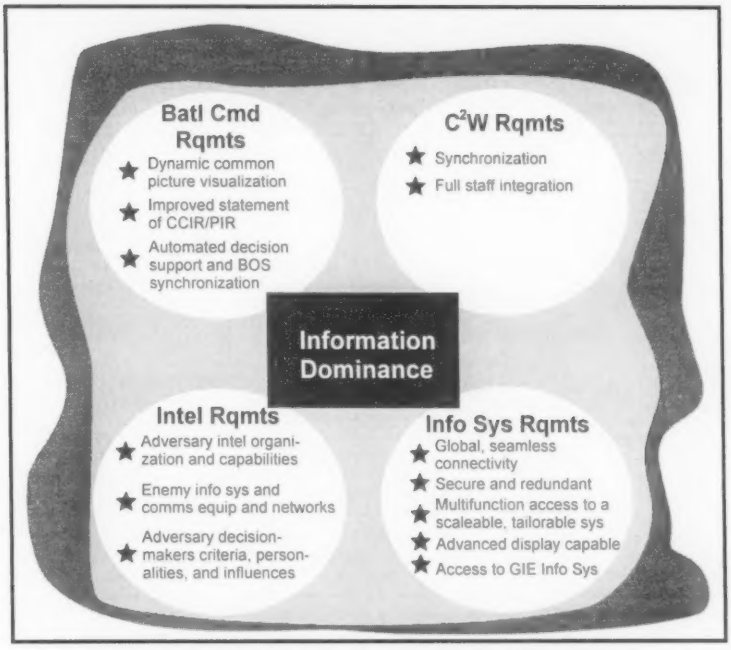


Figure 2. Requirements for Information Operations.

Planning. IO planning is a multifunction endeavor in which many players have a role. Each battlefield function will have information requirements, and these will be met by intelligence staffs and operators, and transmitted over an information system planned by communicators. For the most part these aspects of the IO planning process (information and information systems) are already an integral part of the Army planning process. It is C^2W that needs more definition. C^2W planning, while it occurs in the context of the overall planning process, does have a process of its own. **FM 100-6** establishes a deliberate methodology for planning C^2W, and that methodology must be followed to assure full integration with the overall plan.

Training. None of what has been written above can happen unless our soldiers and leaders are trained to "make it happen." Several recommendations for training the evolving Army to maximize the impact of IO came to light as a result of the wargame. They include—

- ☐ An across-the-board cultural change. Information operations are not stand-alone operations. They cross all BOS and touch the operations of all soldiers. There must be a cultural change throughout the Army that recognizes the importance of the information environment, and the impact of our ability to manage and effect that environment. The impact of IO must be made clear to all soldiers, through classroom instruction and, more importantly, ensuring information plays a role in all exercises.
- ☐ Leader training. Today's tactical Army leaders, brigade and division commanders, must be taught how to visualize the information battlespace, how to clarify information requirements and establish C^2W objectives. In addition, they must have a basic understanding of the tools the C^2W can lever-

age to assist them accomplish their mission, and the requirements they can and must place on the information system that supports their units.

- ☐ Future leaders must be trained as well. By establishing a training program that teaches the doctrine and concepts of IO to all officers and noncommissioned officers, the Army can further the cultural change, and more important, can enable current staffs and future leaders to use IO to its fullest.
- ☐ Specific skill training. The requirements of IO are not just a cultural change. There are some hard skills associated with its execution as well. The wargame players discussed these hard skills and the training that must be established if the skills are to populate the force. Specific skill training was discussed in two areas: IO and C^2W planning (staff process, methodologies and supporting technology) and decision modeling (including studying the adversary's decisionmaking process and technologies).

Conclusion

USAIC&FH has shown through the 1995 IO Wargame that IO has application on the tactical battlefield. The wargame was successful in clarifying the doctrine and concepts laid down in **FM 100-6** and other IW and IO documents. Key to this understanding is recognizing that IO is more than C^2 attack, more than "cyberwar," and, at least for the tactical Army, is much different than the strategic information warfare scenarios that are so intriguing to this nation. Army IO is an effort to use the power of emerging technology to better collect and provide information to commanders, and better allow them to C^2 their units. IO is the progression of intelligence, operational staff operations, and information systems into the information age, with the added dimension of C^2W. Information Dominance is the goal.

Endnotes

1. Statement before the Committee On Armed Services, United States House of Representatives Second Session, 103rd Congress, 2 March 1994.

2. Clauswitz, **On War** (Baltimore, MD: Pelican Books, 1832, 1968), Rapoport, Anatol editor, 162 -165.

3. **FM 100-6**, Information Operations (TRADOC, 1995), 2-I.

4. Joint Chiefs of Staff MOP 30, 8 Mar 93 as quoted in **FM 100-6**, 3-1.

5. FM 100-6, 3-1.

6. Huff, Reid, Colonel, U.S. Army: **"White Paper: Information Dominance"** (Fort Huachuca, AZ: U.S. Army Intelligence Center and Fort Huachuca, 1995), 1.

Mr. McConville is in the Army Reserve and a Project Task Manager for GTE Government Systems Corporation. Before leaving active military service, Captain McConville served with the U.S. Army Intelligence Center's Information Operations Task Force. He served in various intelligence assignments during Operations DESERT SHIELD and DESERT STORM. Mr. McConville has a bachelor of arts degree in Government and Politics from George Mason University, and a Master of Science in Strategic Intelligence from the Defense Intelligence College. Readers can reach him at (703) 247-9218, or via E-mail at jmcconville@mtv.gtegsc.com.

Military Intelligence
PROFESSIONAL BULLETIN

Subscription Order Form

Order Processing Code
*5489

Charge your order. It's easy!

VISA MasterCard DISCOVER

Please send me ____ subscription(s) of ____ year(s) for the Military Intelligence Professional Bulletin at $10.00 (Domestic, APO, and FPO); $12.50 (Foreign) per year.

1. The total cost of my order is $____. All prices include regular domestic postage and handling and are subject to change.

2. _____
(Company or personal name)

_____
(Street address)

_____
(Additional address/ Attention line)

_____
(City, State, ZIP Code)

3. Please choose method of payment:
☐ Check payable to the Superintendent of Documents
☐ GPO Deposit Account No: ☐☐☐☐☐☐☐☐-☐☐☐☐
☐ MasterCard ☐ VISA ☐ Discover exp. date _____

Authorization Signature .....

4. Mail to:
Commander, U.S. Army Intelligence Center and Fort Huachuca, ATTN: ATZS-TDL-B, Fort Huachuca, AZ 85613-6000

Land Information Warfare Activity: IO and IW Support to Army XXI

by Staff Sergeant Richard A. Sizer

Operations in the 21st century will be heavily based on knowledge derived from relevant information and intelligence (RII) collected, processed, analyzed and disseminated over a complex global automated system of systems. The evolving military information environment will fundamentally change the way we, the Army, conduct operations in peace and in conflict. IO includes all measures, both offensive and defensive, taken to achieve information dominance. The Army will integrate IO into every aspect of Army XXI.

—General Dennis J. Reimer
Chief of Staff, Army

To meet this military challenge and to institutionalize the integration of information operations (IO) throughout the force, the Army established the Land Information Warfare Activity (LIWA) on 8 May 1995, as part of the U.S. Army Modernization Plan. LIWA provides today's Army commanders an immediate operational capability that may be called upon to integrate the elements of IO and information warfare (IW) into exercises, operational plans, and orders.

Training and Doctrine Command (TRADOC) recently distributed the new Army doctrine, **FM 100-6, Information Operations**. It calls for continuous military operations within the military information infrastructure (MII) that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations. IO includes interacting with the global information infrastructure by exploiting or degrading an adversary's information and decisionmaking capabilities. It also includes acquiring, using, protecting, managing, exploiting, and denying information and information systems. These activities take place within a battlespace established by the MII.

IW has emerged as an essential joint warfighting mission area. The explosive proliferation of information-based technologies significantly impacts warfighting across all phases, the range of military operations, and all levels of war.

The LIWA Mission

The mission of the LIWA is to provide IO and IW support to land component and separate Army commands, both active and reserve, and to facilitate planning and execution of IO. The LIWA is tasked to provide the following types of support to the Army commander:

- ☐ Operational focal point for land IO and IW operational support by deploying field support teams (FST) to the Land Component Commanders (LCCs).
- ☐ Tailored IO and IW intelligence and counterintelligence to support LCCs.
- ☐ Quick reaction area studies to support LCCs.
- ☐ Assistance in TRADOC development and integration of doctrine, training, leaders, organizations, materiel and soldiers (DTLOMS) requirements and tactics, techniques and procedures for IO and IW.
- ☐ Operational insight, lessons learned, and recommendations to TRADOC and HQDA on IO and IW requirements in the Army Modernization Strategy.
- ☐ Assistance in developing and evaluating IO and IW system performance in exercises such as the Advanced Warfighter Experiments (AWEs).
- ☐ Other operational matters associated with IO and IW.

LIWA Organization and Challenges

The LIWA is specifically organized and equipped to provide tailored IO support to the LCCs (see Figure 1). The LIWA provides commanders with technical expertise and equipment that are not resident on the command's general and special staff, and provides responsive technical interfaces with other commands, Service components, and IW centers. When deployed, the LIWA FST becomes an integral part of the command's IO staff that syn-

Address Verification

Due to new postal regulations, we are updating our mailing lists for the ***MIPB***. The Post Office now requires building numbers, street addresses, and nine-digit zip codes. APO addresses should include unit, box, and CMR number as appropriate. Other oveseas or non-U.S. addresses should be complete, including postal and country codes and names. Please review and update your mailing label. If your address is not correct, please notify us by E-mail at martinezc@huachuca-emh1.army.mil. Include your incorrect **and** correct addresses; the subject line must say only **Mrs. Martinez**. You can also call us at commercial (520) 538-1015 or DSN 879-1015, or write us at the address below.

Commander
USAIC&FH
ATTN: ATZS-TDL-P (Mrs. Martinez)
Fort Huachuca, AZ 85613-6000

chronize and execute IO as part of the overall operation. To facilitate special technical support, the FST has a robust reach-back capability that supports the warfighter. Employing both military and commercial communication capabilities, the FST is electronically tethered to the LIWA Support Center. The Support Center functions as the focal point for the LIWA staff and coordinates intelligence, operations, administrative support, and command functions.

The biggest challenge LIWA faces is in providing information assurance and it requires a most diverse effort. It includes expanding the recently established Army Computer Emergency Response Team (ACERT) Coordination Center, mission support operations, and vulnerability analysis of the current and future Army command, control, communications, computers, intelligence (C^4I) systems and networks. Support to Army XXI is a significant part of this information assurance and command and control (C^2) protect effort. In C^2 support of the Army digitization offices and the HQDA Director of Operations, Readiness and Mobilization, the LIWA is tasked to coordinate and oversee the multidisciplined counterintelligence and operational security (MDCI/OPSEC) assessment and force characterization of the new digitized force, Army XXI. This MDCI/OPSEC assessment will focus on essential elements of friendly information of the military automated information systems. The LIWA will also coordinate and oversee all-source collection and analysis efforts of the digitized force to determine the friendly signature profile, and assess system vulnerabilities which may be open to hostile exploitation and attack. Data collection for this overarching effort will be coordinated during both unit training activity at Fort Hood and during its AWE at the National Training Center in early 1997.

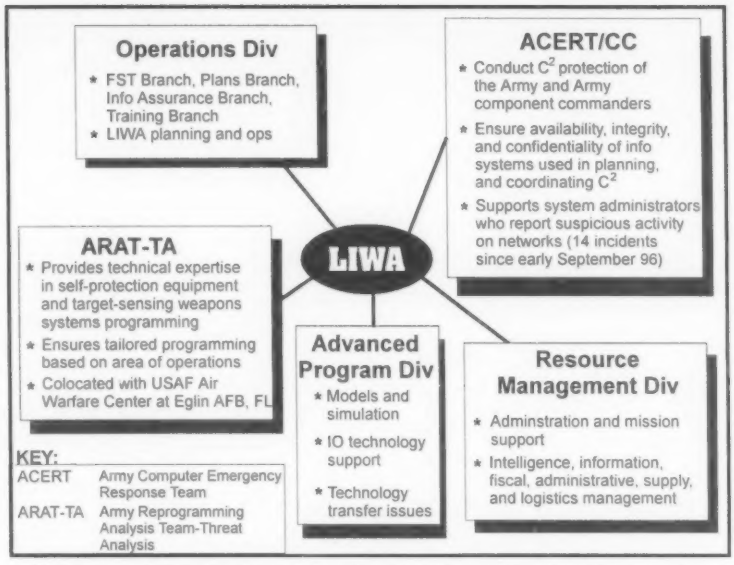

Operations Div
* FST Branch, Plans Branch, Info Assurance Branch, Training Branch
* LIWA planning and ops
ACERT/CC
* Conduct C2 protection of the Army and Army component commanders
* Ensure availability, integrity, and confidentiality of info systems used in planning, and coordinating C2
* Supports system administrators who report suspicious activity on networks (14 incidents since early September 96)
ARAT-TA
* Provides technical expertise in self-protection equipment and target-sensing weapons systems programming
* Ensures tailored programming based on area of operations
* Colocated with USAF Air Warfare Center at Eglin AFB, FL
LIWA
Advanced Program Div
* Models and simulation
* IO technology support
* Technology transfer issues
Resource Management Div
* Adminstration and mission support
* Intelligence, information, fiscal, administrative, supply, and logistics management
KEY:
ACERT Army Computer Emergency Response Team
ARAT-TA Army Reprogramming Analysis Team-Threat Analysis

Figure 1. Organization of the Land Information Warfare Center.

Our reliance on technology creates dependency and vulnerability throughout our basing and information support networks. This generates requirements for **defensive** IW capabilities. However, the same technologies also create vulnerabilities for our adversaries we can exploit using **offensive** IW capabilities. When fully developed and integrated, IW offers enormous potential to support our warfighters.

LIWA's Operational Support Priorities

To assist the LIWA staff in focusing on Army priorities, the Vice Chief of Staff for the Army has provided the following guidance and operational support priorities:

- ☐ Contingency operations.
- ☐ Army XXI initiatives.
- ☐ Combat training center exercises (BCTP, CMTC, JRTC, and NTC).
- ☐ Service school support.
- ☐ Routine operational support.

LIWA tasking for operational support must be submitted through operations channels to the DA Staff, DAMO-ODI, (703) 697-1119, or DSN 227-1119.

Conclusion

A comprehensive IW approach is essential to ensure warfighters have the tools to exploit vulnerabilities while ensuring full access to timely, accurate, and relevant information wherever and whenever needed. The Army Staff, in conjunction with HQ TRADOC, has developed an IO vision and strategy for the Army that address our most urgent needs. Victory Through Information Dominance!

Staff Sergeant Sizer is currently NCOIC for the Intelligence Support Division, LIWA. His assignments include service with the 2d Combat Aviation Brigade, 2d Infantry Division in Korea, and with the Center for Army Tactics at the U.S. Army Command and General Staff College, Fort Leavenworth, Kansas. Staff Sergeant Sizer has an associate of arts degree in Supervisory Leadership from Hawaii Pacific University. Readers can reach him at (703) 706-2266, DSN 235-2266/96 and via E-mail at rasizer@vulcan.belvoir.army.mil

Price Correction

In the October-December 1996 issue of the ***Military Intelligence Professional Bulletin,*** we incorrectly listed the price of **Peacekeeping, Outspoken Observations by a Field Officer** by James H. Allan as $18.95. After further investigation, we discovered the price to be $55.00. We truly regret the error.

INFORMATION WARFARE:
PROTECTING FORCE SUSTAINMENT

by Chief Warrant Officer Two Thomas M. Reardon USA, (Retired)

In the critically acclaimed book, **The First Information War**, contributing editor Colonel Alan Campen USAF, (Retired) emphasizes two key points in the book's preface:[1]

- ☐ The outcome of the Persian Gulf War relied as much on the superior management of knowledge as it did upon performance of people or weapons.
- ☐ History would overlook, misunderstand, misrepresent or perhaps deprecate the key role played by information systems and the people who built them.

Colonel Campen went on to state in his preface that—

> *Western society **and its military components** have come to regard information as a utility; ubiquitous, commonly shared, commonly financed, uncommonly reliable, and always available or **almost always**...forgotten are those infrequent but **terrifying moments** when global finance or air traffic control networks are halted by momentary lapses in computer or human behavior [emphasis added by author].*[2]

The technical accuracy of Colonel Campen's circa 1992 assertions may be subject to some debate within the profession of arms and the automation community. The spirit in which he offered them must be considered as the Army (and the world) moves forward into the age of information. Colonel Campen did not intend to downplay the vital role of the combat soldier—the warrior—in the success of Operation DESERT STORM. To the soldier or Marine on the ground, "war" has only one meaning with very tangible consequences.

Predictions of warfare by exclusive use of computers to cripple national or global economies and infrastructure in lieu of the acquisition of ground by Joint Task Forces ("software over steel"[3]) remains futuristic. This observation regarding the key role of information systems may be subject to discussion since the information support aspect of the Gulf war was viewed as a success. This view may lead us into a false sense of security regarding future operations.

While understanding the human side of closing with the enemy by use of fire-and-movement and fire-and-maneuver, we must take Colonel Campen's words to heart as the "Third Wave"[4] described by Alvin and Heidi Toffler proceeds globally with the force of a virtual tidal wave. Intellectually, this concept seems simple. Computers are here and now, the Army will depend upon them more and more in the future, and we have to account for this change, somehow, in our doctrine and policy.

Information Operations Doctrine

TRADOC has recognized that the experiences of the Persian Gulf War and the reality of the information age requires the development of new doctrine. In an accelerated effort that has reduced timelines from years to months, TRADOC has published **FM 100-6, Information Operations**, dated 27 August 1996.

In the manual's introductory segment, TRADOC recognizes that the Army is—

> *embracing a new era (the so-called "Information Age") characterized by the accelerating growth of information, information sources, and information dissemination capabilities supported by information technology.*[5]

We identify this new era as *"offering unique opportunities as well as some formidable challenges."*[6] These challenges include the "almost always" availability of information services mentioned by Colonel Campen (instead of the "on demand or just in time" assertions made by requirements documents) and the "terrifying moments" described by Colonel Campen.

Current and emerging electronic technologies permit nearly any aspect of a military operation to be made known to a global audience in near-real time

In addition to new doctrine, we must foster new attitudes and beliefs. We focus attention on prosecuting the immediate battle on the ground through the use of high-technology sensors and other information systems in direct support of the warfighter. Perhaps the most "terrifying moments" will occur in the logistics trail that supports the Army's ability to sustain, maintain, and transport the warfighters. "Steel on target" will remain a critical element of modern warfare. Supply and logistics will remain an equally critical element, as it was during the campaigns of Alexander the Great. A special focus on this logistics "tail" must occur during military planning in the age of information especially during exercises and war games where far too often resupply is a "given."

Automated Logistics and Supply Tracking

Using Operation DESERT STORM as an example, the Tofflers related in their book, **War and Anti-War**, that the U.S. Army was able to track via the use of

computers and satellites the huge amounts of logistics required to sustain the force. The numbers are staggering from Operations DESERT SHIELD through DESERT FAREWELL where the Army—[7]

- ☐ Mobilized 550,000 soldiers.
- ☐ Shipped 7,000,000 tons of supplies.
- ☐ Served 122 million meals.
- ☐ Pumped 1.3 billion gallons of fuel.
- ☐ Drove 52 million miles.
- ☐ Maintained 12,575 aircraft.
- ☐ Delivered 32,000 tons of mail.

This tracking was done in a fashion similar to the method used by large commercial shipping companies such as Federal Express and United Parcel Service to keep tabs on hundreds of tons of freight shipped each day all over the world. This success enabled Lieutenant General William Pagonis to state that "...this (was) the first war in modern times where every screwdriver, every nail (was) accounted for."[8]

Certainly one may view the accountability of individual tools and nails as "overkill." The contextual meaning of the remarks by General Schwartzkopf's logistics officer (J4) is both clear and anticipated: computers make the monumental task of sustaining warfighters in a power projection scenario workable and realistic and anticipated. Without reliable automated information systems, the concept of power would no doubt require a relook. Without a doubt, our potential adversaries are not overlooking this dependence on the "reliability" of U.S. automated information systems. The objective of these adversaries is most certainly to turn "reliable" into "not reliable," and thus order into chaos.

Threat to Information Systems

The term "reliable" goes beyond the context of efficient operation according to standards, both mechanical and human. This term must also account for reliable operation under the stress of information warfare (IW) or "a large structured attack with strategic intent against the United States could be prepared and exercised under the guise of unstructured activities."[9] Given that a significant amount of U.S. Army communications (voice and data) travel over the public switched network (to include commercial leased satellites), we cannot discount national IW issues as being out of the Army's "lane." More than 100 nations have an IW capability, and more than 50 are known to target the United States.[10] For example, Chinese military leaders have concluded that victory in any future war will ultimately depend on the capability of the People's Liberation Army's (PLA) to effectively wage IW in all phases of the conflict (not limited to command and control (C2)).[11] This lack of limitations indicates an appreciation by the PLA (and certainly by others) of the value that information systems add in addition to those used to command and control lethal manuever forces are high-value IW targets.

History will no doubt verify...that superior management of knowledge will dictate the winners of battles

Traditional military thinking regarding protection of vital assets focused on strong physical barriers to keep out traditional battlefield threats and threats to rear area operations. In the information age, "physical" (in the traditional and doctrinal sense) alone is not adequate. An excellent example is a story cited by Leonard Lee in his book **The Day the Phones Stopped—How People Get Hurt When Computers Go Wrong**.[12] He discusses what happened to the operations of American Airlines and that company's Sabre reservation system in spite of strong physical barriers certainly a "terrifying moment" (which lasted 12 hours). Despite state-of-the-art physical security including retinal scans and a bullet-proof entryway, the system was laid low. A software error caused by the installation of a new memory disk drive fully disabled the system for 12 hours. In an IW scenario, the "what if's?" of an occurrence like this are endless.

IW Technology

The impact of technology has not been limited to military applications. Most of the high technology needed to employ IW techniques against U.S. Army operations is also readily accessible to thugs, despots, and fanatics[16] as well as foreign military and commercial interests. The Department of Defense is required by Congress (and common sense) to rely on commercial off-the-shelf (COTS) software for a variety of sound fiscal reasons. While use of COTS software is cheaper and sensible in one respect, we must weigh the potential IW impact as well.

Speaker of the House Newt Gingrich posed an interesting and thought-provoking question during a presentation at the National Defense University in February 1995 when he asked *"...what does it mean that Madras, India, is the second largest center of software development in the world?" The Speaker's remarks, of course, refer to the potential impact foreign-origin software may have on U.S. computers supporting military operations in an IW situation.*

Information technology has made possible the compromise or corruption of critical information and the disruption of information services in a matter of seconds from the threat source on the other side of the continent or the world. This is a far cry from traditional frames of reference such as boundaries, lanes, and ranges of weaponry, supplemented by biographical data on opposing com-

manders, knowledge of enemy ground order of battle, and doctrine to assist in battlefield success.

IW and the Sustaining Base

The Army is a member of the global information environment (GIE). The Army shares this "space" with the national and international news media, academia, commerce, drug cartels, industry, and more. The GIE is interactive, and pervasive in its presence and influence—it has no real "master." Current and emerging electronic technologies permit nearly any aspect of a military operation to be made known to a global audience in near-real time. This factor, coupled with the ready availability of IW techniques to foreign governments, terrorists, criminal elements, or anyone else willing to pay the bill, removes the ability to cripple armies from the sole domain (and control) of the traditional warrior in uniform.

Given this "global reach" and the concept of Force XXI (which envisions the use of automation to enable deployed forces to "reach back" to depots in the continental United States), we must not overlook the data streams and networks carrying requisitions, manifests, orders and so forth, in the seemingly mundane area of combat service support. Protecting C^2 on the battlefield is important, but the force has to be on the field to maneuver and to face the enemy. IW can delay that presence if the networks and systems supporting the critical yet often overlooked sustaining base are not incorporated into Army information operations planning. Overlooking the impact of IW on such seemingly "automatic" chores as troop movement and sustainment can lead to enemy success without firing a shot. This planning process must include—

- ☐ Knowledge and appreciation of the threat. Fortifications, in the traditional sense, are no real barriers to this new threat. Familiar terms such as "thickness," "depth," "steel," and "armor" must share thought-space with new terms such as "information systems security" and not-so-new terms like "operations security."
- ☐ Appreciation that the Army is a member of the GIE with all its attendant risks. The information requirements of our warfighters and sustainers are but a mere speck in this "new universe" and our influence is limited.
- ☐ Understanding that the automated information systems supporting the processes that mobilize, train, deploy, maintain, and sustain the force are choice IW targets. U.S. soldiers remain the best in the world. However, their ever-growing reliance on automation that works through the GIE to provide logistics and supply makes this automated "tail" an obvious choice for IW activity. Such activity can come from any spot on the globe at the speed of a keystroke.
- ☐ Provision for exercising IW plans, tactics, and techniques to protect vital automated systems supporting sustaining base activities. The axiom that we will fight as we train applies to those activities that will sustain our forces. That long line of communication through "cyberspace" presents awesome challenges and opportunities for exercise planners to test our mettle in IW.

History will no doubt verify again and again Colonel Campen's assessment that superior management of knowledge will dictate the winners of battles. Transformed into capabilities, information is the currency of victory.[13] It is debatable whether information systems such as the Sustaining Base Information Services and Reserve Component Automated System will be recognized with the same reverence as the names Colt, Springfield, Remington, and Garand. What is not subject to debate is the fact that the Army's commitment to reliance upon automation technology to support successors of Lieutenant General Pagonis (and, ultimately, the warfighter) has gone way past the point of no return. How history remembers information systems (and the people who design, operate, and maintain them) will depend upon how seriously we take the contemporary threats to these systems.

Endnotes

1. Colonel Alan Campen USAF, (Retired), Contributing Editor, **The First Information War**, Armed Forces Communications and Electronics Association (AFCEA) Press, 1992.

2. Ibid, vii.

3. Alvin and Heidi Toffler, **War and Anti-War, Survival at the Dawn of the 21st Century**, Little, Brown, and Company, 1993, frontspiece. The agricultural age was first, followed by the industrial age; the information age is the third wave.

4. Ibid, 9.

5. Doctrine Review Advisory Group (DRAG) Draft **FM 100-6, Information Operations**, Headquarters, Department of the Army, October 1995, iii.

6. Ibid.

7. Lieutenant General William G. Pagonis with Jeffrey Cruikshank, **Moving Mountains Lessons in Leadership from the Gulf War** (Boston: Harvard University Press, 1992), frontspiece.

8. Toffler, 78.

9. Office the Under Secretary of Defense for Acquisition and Technology, **Report of the Defense Science Board Summer Study Task Force on Information Architecture of the Battlefield**, October 1994, 24.

10. Ibid.

11. National Ground Intelligence Center (NGIC), NGIC-1100-55D-96, **China's Focus on Developing Electronics Technology Applicable to IW (U)**, by Dr. E. McKenzie, 8 December 1995.

12. Leonard Lee, **The Day the Phones Stopped--How People Get Hurt When Computers Go Wrong** (New York: Donald I. Fine, Inc., 1992), 134-135.

13. **FM 100-6**, iii.

Mr. Reardon is an Intelligence Operations Specialist with the Office of the Deputy Chief of Staff for Intelligence, U.S. Army Signal Command (formerly called the Information Systems Command) at Fort Huachuca, Arizona. He is a graduate of Chaminade University of Honolulu, with a bachelor of arts degree in General Studies. Readers can contact him at (520) 538-6255, DSN 879-6255, and via E-mail at reardont@huachuca-emh12.army.mil.

Roster of Key Intelligence Personnel

HQDA

LTG Paul E. Menoher, Jr.
DCSINT
DSN: 225-3033
C: (703) 695-3033
menoher@Pentagon-hqdadss.army.mil

Major Commands

FORSCOM

LTC John D. Frketic
DCSINT
DSN: 367-6440
C: (404) 669-6440
frketicj@ftmcphsn-emh1.army.mil

AMC

COL Austin J. Kennedy, III
DCSINT
DSN: 767-8136
C: (703) 617-8136/4
kennedya@alexandria-emh1.army.mil

Eighth U.S. Army

COL Robert Staggers
G2
DSN: (315) 723-3918
C: 011-822-7913-3918

Signal Command

COL Peter Huisking
DCSINT
DSN: 879-6621
C: (520) 538-6621
huiskingp@huachuca-emh12.army.mil

INSCOM

BG John D. Thomas, Jr.
CDR
DSN: 229-1603
C: (703) 706-1603
cg@vulcan.belvoir.army.mil

MDW

LTC Willie Lane
DCSOPS, Chief, Intelligence
DSN: 335-2845
C: (202) 685-2845/11

Space and Strategic Defense Command

COL Jimmy L. Slade
DCSINT
DSN: 327-2053
C: (703) 607-2053
sladej@ssdcw.usassdc.army.mil

TRADOC

COL Nicholas P. O'Dawe
DCSINT
DSN: 680-3113
C: (804) 727-3113
odawen@monroe-emh10.army.mil

USAIC&FH

MG Charles W. Thomas
CDR
DSN: 821-1140
C: (520) 533-1140
thomasc@huachuca-emh1.army.mil

USARC

COL Marcel Fauk
DCSINT
DSN: 1-800-359-8483 ext 7900
C: (404) 629-7900
fauk@ftmcphsn-emh1.army.mil

USARPAC

COL Martin G. Kloster
DCSINT
DSN: (312) 438-9214
C: (808) 438-9214
klosterm@shafter-emh3.army.mil

USARSO

LTC Charles Atkins
DCSINT
DSN: 313 287-3062
C: 011-507-285-3179/3062

USASOC

COL Daniel Morris
DCSINT
DSN: 239-6302/1
C: (910) 432-6302

PERSCOM

LTC Gary Royster
Chief, MI Off Branch
DSN: 221-0145
C: (703) 325-0145
roysterg@hoffman-emh1.army.mil

USAREUR

COL John C. Hammond
DCSINT
DSN: 370-8854/9002
C: 011-49-6221-57-8854
carter@dcsint.hqusareur.army.mil

U.S. Armies

First

LTC Roy H. Adams, Jr.
DCSOPS, Chief, I&S
DSN: 797-7550
C: (404) 362-7550

ARCENT/Third

COL William Moore
G2
DSN: 572-4803
C: (404) 752-4803

Fifth

Mr. Gonzalo Gallegos
Chief, I&S
DSN: 471-1702
C: (210) 221-1909/1702

Corps

I Corps

COL Dave Oberst
G2
DSN: 357-0293
C: (206) 967-0293
oberstd@lewis-ems1.army.mil

III Corps

COL Nicholas P. Grant
G2
DSN: 737-2202
C: (817) 287-2202
grantn@hood-emh3.army.mil

V Corps

COL Maxie L. McFarland
G2
DSN: (314) 370-5200/1
C: 011-49-6221-57-5200/1
mcfarlanm@victory6.vcorps.army.mil

XVIII (ABN) Corps

COL Richard Allenbaugh
G2
DSN: 236-5716
C: (919) 396-5716/08
allenbar@bragg-emh5.army.mil

Divisions

1 AD

LTC Harold L. Bakken
G2
DSN: (314) 490-6122
C: 011-49-671-609-6122
g2sec@iron2.1ad.army.mil

1 CAV

LTC Gus E. Greene
G2
DSN: 737-3983/6202
C: (817) 287-3983
greeneg@hood-emh3.army.mil

1 ID (M)

LTC Jeffrey N. Rapp
G2
DSN: (314) 350-6242
C: 011-49-931-889-6242
aetvbgb@email.hq.1id.army.mil

2 ID

LTC Foster Payne
G2
DSN: (315) 732-8851
C: 011-82-351-870-8851
eaid-gi-g2@emh2.korea.army.mil

3 ID (M)

LTC Kenneth H. Boll
G2
DSN: 870-2202
C: (912) 767-2202
bollk@emh5.stewart.army.mil

4 ID (M)

LTC John R. Brooks
G2
DSN: 737-9218
C: (817) 287-9218
brooksj@hood-emh3.army.mil

10 MTN (L)

LTC Charles F. Sardo
G2
DSN: 341-5405/7508
C: (315) 772-5405
sardoc@drum-emh3.army.mil

25 ID (L)

LTC Charles Borg
G2
DSN: (315) 455-4002
C: (808) 655-4002
acofsg2@schofield-emh1.army.mil

82 ID (ABN)

LTC Thomas H. Tutt, II
G2
DSN: 239-2252/0622
C: (910) 432-2252
tuttt@emh5.bragg.army.mil

101 (AASLT)

LTC Gerald N. Vevon, Jr.
G2
DSN: 635-4802/3022
C: (502) 798-4802/3022
vevong@campbell-emh5.army.mil

Separate Brigades

1 Bde, 6 ID

CPT Michael Chinn
S2
DSN: 317 353-6022
C: (907) 353-6022

3 Bde, 1 AD

MAJ Steven Eldridge
S2
DSN: 856-9998

3 Bde, 3 ID

CPT Mitchell Bohnstedt
S2
DSN: 784-1462
C: (404) 544-1462

11 ADA Bde

MAJ Sandra Gallardo
S2

DSN: 978-1370/2480
C: (915) 568-1370

94 ADA Bde
CPT Nichole Redington
S2
DSN: (314) 348-6555
C: 011-49-6151-69-6555

Regiments

2 ACR
MAJ William B. LeWallen
S2
DSN: 863-0572/77
C: (318) 531-0572/77

3 ACR
MAJ William J. Cojocar
S2
DSN: 691-9591/4368
C: (719) 526-9591
cojocarw@carson-cav3.army.mil

Corps Spt Cmds

13th Corps Spt
MAJ Daniel Godfrey
G2
DSN: 737-5110/2596
C: (817) 287-5110

Special Operations

USAFC
MAJ Richard W. MacDougall
G2
DSN: 239-7853/7865
C: (910) 432-7853/7865

1 SFG (A)
MAJ Roger Fortier
S2
DSN: 357-8622/21
C: (206) 967-8622/1

3 SFG (A)
MAJ Stephen C. Kachmar
S2
DSN: 239-9065
C: (910) 432-9065/5303

5 SFG (A)
MAJ Robert S. Henderson
S2
DSN: 635-2355/2899
C: (502)798-2355

7 SFG (A)
MAJ Edwin W. Passmore
S2
DSN: 239-7629/2227
C: (910) 432-2227
passmore@usasoc.soc.mil

10 SFG (A)
MAJ Byron Castleman
S2
DSN: 883-1814

19 SFG (A)
MAJ Tuck A. Miller
S2
C: (801) 576-3737

20 SFG (A)
MAJ John W. Grimes
S2
C: (205) 951-5303

4 PSYOPS GP
MAJ James Callahan
S2
DSN: 239-4181/5216
C: (910) 432-5216

75 Ranger Regiment
MAJ Raymond C. Mallgren
S2
DSN: 835-5765
C: (706) 545-5765
rmallgren@soc.mil

160 Special Operations
COL Dell L. Dailey
CDR
DSN: 635-1749
C: (502) 798-1749

Other

USASETAF
LTC Rex E. Dudley
G2
DSN: 314 634-7423/7702
C: 011-39-444-5174-23
aesegi@email.vicenza.army.mil

USARSPACE(Fwd)
LTC William D. Kendrick
DCSINT
DSN: 692-8752
C: (719) 554-8752
kendrickw@spacecmd-emh2.army.mil

USARJ
COL Michael J. Diver
DCSINT
DSN: (315) 263-8010/8580
C: 011-81-311-33-8010

USARAK
Mr. Skip Stiglich
SIO
DSN: (317) 384-2208
C: (907) 384-2208
stiglichf@richardson-emh2.army.mil

Defense Language Inst.
COL Daniel D. Devlin
Commandant
DSN: 878-5312
C: (408) 242-5312

U.S. Army and Ft. Riley
LTC Steven L. Lovitt
G2
DSN: 856-3987
C: (913) 239-3989
afzngs@riley.emh1. army.mil

U.S. Army Armor Center and Fort Knox
Mr. Shelby C. Roberts
Chief, Security Division
DSN: 464-7050
C: (502) 624-7050
robertss@knox-emh1.army.mil

Joint Commands
J2/Senior Army Element

EUCOM
COL Gerald Joyce
Chief, Collection Division
DSN: (314) 430-7314
C: 011-49-711-680-7314

USACOM
COL Larry L. Miller
Deputy Dir for Intelligence
DSN: 564-6626
C: (804) 444-6626
j2a@limsmail.acoms.smil.mil

CENTCOM
BG Robert W. Noonan
J2
DSN: 968-6265
C: (813) 828-6265
noonanrw@ccfs.centcom.mil

SOCOM
COL Donald R. Faint
SOJ2
DSN: 968-3733
C: (813) 828-2144

TRANSCOM
LTC Susan Rhein
Chief, Plans and Systems Div
DSN: 576-1870
C: (618) 256-1870

SOUTHCOM
BG Robert A. Harding
J2
DSN: (313) 282-6980
C: 011-507-82-6980/3313

NORAD/SPACECOM
COL Joseph M. Blanco
CDR, J2W
DSN: 692-3831
C: (719) 554-5212

STRATCOM
COL Terrance E. Nelson
Chief, Force Assessments
DSN: 271-3251
C: (402) 294-4530

PACOM
COL Bruce L. Meisner
Deputy J2
DSN: (315) 477-7324
C: (808) 477-7324
pdmeibl@cinc-mail.pacom.ic.gov

SHAPE/NATO
COL Thomas Roeber
Chief, Assessment, Yugo Cell
DSN: (314) 423-3751
C: 011-32-6544-3751

USFK
COL Wayne M. Hall
J2
DSN: (315) 725-6312/4310
C: 011-822-791-54-4310

Joint Intelligence Centers

JICPAC
COL Jeffrey E. Burton
Deputy CDR
DSN: (315) 474-8390/9192
C: (808) 474-8390/9192
jburton@jic-mail.pacom.ic.gov

JAC
COL Philip Marcum
CDR
DSN: (314) 268-2546
C: 011-480-84-2546

Joint Field Support Center
COL R. John Cully, Jr.
CDR
DSN: 923-2134
C: (301) 677-2134

Separate MI Companies

F Co, 110th MI Bn/ 6 ID
CPT Christopher Tatarka
CDR
DSN: (317) 353-9671
C: (907) 353-9671

66 MI Co (CEWI)/ 3 ACR
MAJ Patrick Ahrens
CDR
DSN: 691-1962
C: (719) 524-1962

502 MI Co/ 2 ACR
CPT Thomas L. Evans
CDR
DSN: 863-0779

511 MI Co (CEWI)/ 11ACR
CPT Bruce Perry
CDR
DSN: 470-3921
C: (619) 380-3921

MI Groups/ Brigades

66th MI Group
COL Barbara G. Fast
CDR
DSN: (305) 435-6611
C: 011-49-821-540-7582

iagpa-co@ausburg-emh1.army.mil

111 MI Bde (TNG)
COL Rodney Medford
CDR
DSN: 821-1154
C: (520) 533-1154
medfordr@huachuca-emh1.army.mil

201 MI Bde (CEWI)
LTC John Hall
CDR
DSN: 357-3041/2440
C: (206) 967-3041

205 MI Bde
LTC Michael Fox
CDR
DSN: 357-6241
C: (206) 967-6241
foxm@lewis-emh2.army.mil

504 MI Bde (CEWI)
COL James A. Marks
CDR
DSN: 738-1329
C: (817) 288-1329
marksj2@hood-emh3.army.mil

525 MI Bde (CEWI)
COL Keith B. Alexander
CDR
DSN: 236-3209/6084
C: (919) 396-3209
alexandk@emh5.bragg.army.mil

650 MI Group
COL Donald D. Woolfolk
CDR
DSN: (314) 423-4598
C: 011-32-65-44-4598

718 MI Group
COL Charles H. Berlin, III
DSN: (314) 441-5964/3827
C: 011-49-8061-38-5966/5745

902 MI Group
COL Ben L. Elley
CDR
DSN: 923-6991
C: (301) 677-6991
elleyb@meade-emh1.army.mil

Intelligence and Security Command Brigades

470 MI Bde
COL Ronald Burgess, Jr.
CDR
DSN: (313) 285-4012
C: 011-507-285-4012
rburgess@usarso-lan1.army.mil

500 MI Bde
COL Jer D. Get
CDR
DSN:P (315)263-3986
C: 011-81-3117-633819
iapd-cdr@zama-emh1.army.mil

501 MI Bde (EAC)
COL Charles W. Alsup
CDR
DSN: (315) 723-6069
C: 011-822-7916-6069
iabdk-cdr@emh1.korea.army.mil

513 MI Bde
COL John C. Green
CDR
DSN: 780-9178
C: (706) 791-9178

702 MI Bde
COL Patrick J. Gagan
CDR
DSN: 780-9175
C: (706) 791-9175
gaganp@emh1.gordon.army.mil

703 MI Bde
COL Robert R. Murfin
CDR
DSN: (315) 455-3301
C: (808) 655-3301
703cdr@schofield-emh1.army.mil

704 MI Bde
COL Michael J. Blythe
CDR
DSN: 923-0364
C: (301) 688-4708
blythem@meade-emh1.army.mil

Divisional MI Battalions

101 MI Bn
LTC Mark Volk
CDR
DSN: (314) 350-7393
C: 011-49-931-889-7393
aetvbmi-cdr@email.hq.1id.army.mil

102 MI Bn
LTC Henry O'Brien
CDR
DSN: (315) 732-6577
C: 011-82-351-870-6637
eaid-mi-co@emh2.korea.army.mil

103 MI Bn
LTC James M. McCarl
CDR
DSN: 870-8222
C: (912) 767-8222
afzp-vmi-c@stewart-emh4.army.mil

104 MI Bn
LTC Steven L. Campbell
CDR
DSN: 738-3910
C: (817) 288-3910
campbells@hood-emh3.army.mil

110 MI Bn
LTC Brian A. Keller
CDR
DSN: 341-8088/86
C: (315) 772-8086/88
kellerb@drum-emh1.army.mil

125 MI Bn
LTC Kent Thew
CDR
DSN: (315) 455-4916/5
C: (808) 655-4916/5
comi25@schofield-emh1.army.mil

311 MI Bn
LTC Patrick McNiece
CDR
DSN: 635-5554
C: (502) 798-5554

312 MI Bn
LTC Patrick L. Neky
CDR
DSN: 738-7900
C: (817) 288-7900
nekyp@hood-emh3.army.mil

313 MI Bn
LTC Theodore C. Nichols
CDR
DSN: 239-1635/8500
C: (919) 432-1635
nicholst@bragg-emh5.army.mil

501 MI Bn
LTC Kevin D. Johnson
CDR
DSN: (314) 334-5755
C: 011-49-61-336-9867
johnsonk@email.badkreuznach.army.mil

Separate Training Battalion

229 MI Bn, DLI
LTC Jason Ploen
CDR
DSN: 878-5591
C: (408)242-5591
ploenj@pom-emh1.army.mil

U.S. Army Intel Center and Fort Huachuca

<USER NAME>...@huachuca-emh1.army.mil

USAIC&FH
MG Charles W. Thomas
CDR
DSN: 821-1140/47
C: (520) 533-1140/47
thomasc@...

BG John W. Smith
Deputy CDR,
DSN: 821-1141/48
C: (520) 533-1141/48
smithj@...

Dir of Operations, Training & Doctrine
COL Robert C. White, Jr.
DIR
DSN: 821-2928/3055
C: (520) 533-2928/3055
whiter@...

Dir of Combat Devel
Michael W. Powell
Actg DIR
DSN: 821-3841/2415
C: (520) 533-3841/2415
powellm@...

Battle Cmd Battle Lab (Huachuca)
COL Reid S. Huff
Deputy DIR
DSN: 879-0570/4661
C: (520) 538-0570/4661
huffr@huachuca-emh30.army.mil

TSM ASAS
COL Lester F. McConville
DSN: 821-3504
C: (520) 533-3504
mcconvillec@...

TSM GBCS/Ground Sys
COL Eugene J. Komo, Jr.
DSN: 821-5579/5850
C: (520) 533-5579/5850
komoe@...

TSM Joint STARS
COL Michael H. Gourgues
DSN: 821-5301/5201
C: (520)533-5301/5201
gourgues@doim6.monmouth.army.mil

TSM UAV
COL Ronald W. Wilson
DSN: 821-2165/2971
C: (520) 533-2165/2971
wilsonr@...

TSM TENCAP
CW2 Charles S. Montgomery
DSN 821-4610/4
C: (520) 533-4610/4
montgomerys@...

Information Warfare: Good News and Bad News

by Major Keith D. Anthony, USAR

The views expressed in this article are those of the author and do not reflect the official policy or position of the National Air Intelligence Agency, Department of Defense, or the U.S. Government.

The chief objective of information warfare is to achieve information superiority over an adversary. It might mean more information; it definitely does mean better information. IW means making sure our information is reliable and accurate. At the same time, IW means denying information superiority to an adversary. This could mean denying information or manipulating the information available to an adversary. The playing field is "info-space"—the collection of all things involved in generation, gathering, processing, storage, and transmission of information. IW holds that the information a nation's military has available to make a decision will, to a large extent, determine its activities. If that information can be controlled, so can the resulting military actions.

Always a tool of war, information has now become a target of war as well

IW reflects the changing nature of warfare.[1] It has evolved to the extent that for most nations, and especially the United States, information technology is inherent in their war-fighting capabilities. For some nations, information technology is used very little within their military. For these nations, the weapons of IW provide an offensive force multiplier against information technology-dependent opponents.

However, IW is broader than foreign nations. The same tools and techniques are available to organized crime, terrorists, and other groups. IW applies to all phases of a conflict. It affects far more targets than military equipment and personnel. Critical infrastructure components, such as the power grid, telecommunications networks, and transportation systems all rely on computer networks for their operation.

The Fragile Infrastructure

A recent government report estimates that as many as 250,000 DoD computer systems were attacked last year.[2] The report also concludes that 65 percent of these attacks were successful, and that the number of attacks doubles each year.[3] Computer attacks are not a new phenomenon. They have been occurring since the beginnings of the Internet. However, in the context of IW, they are becoming increasingly significant.

Why should the military care about these attacks? Are they anything more than just some misguided computer geeks with too much time on their hands? Military history has many examples of how information has been used in conflicts. It has always been sought; sometimes it has even been used effectively, and sometimes it has been vital. The common thread, though, has been that physical engagements were still necessary to impose one's will upon the enemy. IW changes the rules. With the appropriate information, it may now be possible to accomplish objectives without the use of military force.[4] On the other hand, denied the use of required information and information technology, we may be prevented from using military force to accomplish our objectives. Always a tool of war, information has now become a target of war as well. Information and the technology used to generate, transmit, process, store, and manipulate it, may very well have become the primary means of obtaining an offensive or defensive advantage.[5]

The U.S. military is probably the world's best-postured fighting force in terms of its use of information technology. It has a vast and complex information infrastructure with more than 2.1 million computers, 10,000 local computer networks, and 100 long-distance networks. The DoD uses information technology for—

- ☐ Designing weapons.
- ☐ Identifying and tracking enemy targets.
- ☐ Paying soldiers.
- ☐ Mobilizing reservists.
- ☐ Managing supplies.
- ☐ A myriad of other essential activities.

Information systems and computer-based telecommunications networks provide the very basis of our war-fighting capability. However, this is a double-edged sword because the DoD must also protect this information infrastructure. Our dependence on information technologies also makes us susceptible to its vulnerabilities. Computer attacks like those mentioned above illustrate the degree to which DoD computer systems are being targeted. The success rate illustrates the potential damage that could be done by organized foreign nationals, terrorists, or "hackers". As a minimum, we must expend resources on repairing the damage done by the attacks; at worst, parts of our information infrastructure could be disrupted or rendered inoperative by attacks.

What is this "information infrastructure" and why should we care about it? The information infrastructure is all of the systems and equipment used to transmit, store, and process information that DoD needs to accomplish its mission. Much of this infrastructure is the same as that used by the civilian world. To operate more efficiently, DoD has been rapidly moving away from isolated and stand-alone information systems to a globally integrated information structure. In doing so, it has linked together thousands of computers with the Internet as well as other networks, and increased its dependence on computer and network technology to do its basic functions.

This raises a number of concerns. What if—

- ☐ These systems or large parts of them were destroyed?
- ☐ They were merely made unavailable for a time period?
- ☐ The information they contained was compromised?
- ☐ Random parts of that information were corrupted or made unreliable?
- ☐ Malicious software was introduced into these systems?
- ☐ An enemy decided to exploit design flaws in the infrastructure on which we depend?
- ☐ An enemy was in control of a computer system on which we used to help make critical battlefield computations?
- ☐ A hostile foreign nation built all of the microelectronic components we used in an important military system?

Recently there has been a vivid example of just such exploitation. By exploiting a design flaw in the Internet protocol (IP), attackers recently "flooded" an eastern United States Internet service provider's host computer with bogus requests for service. Since the computer had to respond to these requests, it was unable to service legitimate ones. This is known as a denial-of-service (DOS) attack, since it denied service to those dependent on that computer. The attack was based on information widely available in some of the "computer-underground" publications.[6] It painfully illustrated a vulnerability of any computer that uses the IP protocol, that is any computer connected to the Internet.[7]

Government agencies have acknowledged that potential adversaries have been developing bodies of knowledge about DoD's and other U.S. systems and about methods to attack these systems. Many methods and tools to accomplish attacks are widely available.[8] These methods include sophisticated computer viruses and automated attack routines, and typically allow adversaries to launch untraceable attacks from anywhere in the world. Official estimates show that more than 120 countries are developing such computer attack capabilities.[9]

Long the toys of computer hackers, these tools and methods are becoming the weapons of IW. A more important point is that these tools are available cheaply and to the same degree to terrorists, organized-crime, and potential military enemies. In fact, for a number of years now, the technology has existed for a person of moderate intelligence to bring down large portions of the Internet.[10]

Information Warfare Russian and Chinese Style

It is probable that foreign nations are developing doctrine and tactics for IW and assembling IW "weapons." Russia is one such nation. While no official statement on IW by the Russian Ministry of Defense or General Staff has been found, statements by a number of senior military officers give us some insight into Russian thinking on the topic. Senior Russian officers speak of "computer virus warfare," where they see several different virus types with which they must contend:

- ☐ The "Trojan Horse" virus remains idle for a certain period of time and then causes catastrophic destruction of the system.
- ☐ The "force quarantine" virus knocks out the program of the unit into which it was planted.
- ☐ The "overload virus" quickly spreads through a system and gradually slows its operation.
- ☐ The "sensor virus" penetrates a preplanned sector of a computer's data-storage area and destroys the data bank and its information at a critical moment.

Another key Russian concept is that of disinformation, which follows closely the Soviet concept of *maskirovka* of the Cold-War days.[11]

Chinese writers also recognize that this significant change has occurred in the nature of warfare, even calling it a military revolution. In the words on one Chinese scholar—

Information technology is the nucleus and foundation of this revolution, for it is information and knowledge that bring change to the old practice that the military strength of an army was measured simply by the number of its armored divisions, air force wings, and aircraft carrier groups. Today, a number of invisible forces need to be taken into consideration, which include the calculation capacity, the telecommunications volume, and the reliability and real-time reconnaissance ability of relevant systems.[12]

While China's preparation for warfare in this new era is just getting underway, they recognize many of the important questions which all nations must consider. For example—

- ☐ Precisely how will this military technological revolution take place?
- ☐ Will military forces maintain their old structures and merely adapt information technologies to those structures? Or will information technologies become the structure and framework upon which entire military forces are built?
- ☐ Also, what about the underdeveloped countries of the world? Will the armies of these countries complete the transformation to mechanized warfare before considering a shift toward IW? Or will they skip a generation in military thought and practice?
- ☐ What primary force will drive the evolution and deployment of a nation's military forces, technological development, or tried and tested military doctrine?[13]

The Chinese recognize two ironies which surround IW. First, it seems that the further technology develops, the easier it becomes to catch up. Underdeveloped countries can very often find shortcuts for information technology development and attain similar standards within a far shorter period of time. It may be far cheaper for an underdeveloped na-

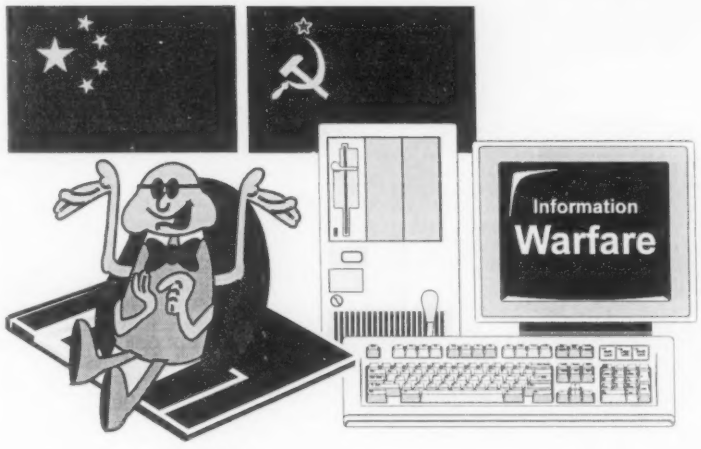
tion to exploit a technological weakness than for a more advanced nation to develop and deploy the system that has the weakness. Second, the further information technology develops, the more fragile and vulnerable it becomes. Note that modern software is now typically so complex that it is impossible to thoroughly test it.[14]

Often cited as the "first information war," Operation DESERT STORM created an appetite and fueled expectations for military forces intent on dominance of the information spectrum (as is the objective of IW). U.S. forces did just that in DESERT STORM, creating an information differential that seemed to paralyze the enemy. However, it did so only after five months of gathering together a kludge of Free World sensing, telecommunications, and intelligence systems not designed for joint operations, and then tinkering with it while the enemy was content with inactivity. Coalition ingenuity, enemy inactivity, and modern information technology changed an unfamiliar battlefield into one of military confidence, precision, and efficiency. Instead, imagine a conflict where missile batteries receive no firing solutions, where Tomahawk launch platforms receive no targeting instructions, where an aircraft's situational awareness screens go blank, or where a computer virus makes a unit's mission planning computers useless.[15]

The Weapons of IW

The above viruses are but a few of the potential IW weapons. Others include traditional weapons which might be used to destroy information systems. Still others include other types of—

- ☐ Malicious software.
- ☐ "Chipping" (manipulating the functions on microelectronic circuitry).
- ☐ Software "back doors" (which allow unauthorized access to programs).
- ☐ Electromagnetic weapons.
- ☐ Destructive microbes and chemical agents.



- ☐ Van Eck radiation (which allows monitoring of radio emissions from electronic devices).
- ☐ Cryptography.
- ☐ Spoofing (faking the identity of a legitimate user).
- ☐ Video "morphing."
- ☐ Psychological operations (for example, by controlled release of information).
- ☐ Attacks on financial institutions, disruption of air traffic control, and others.

Many of these "weapons" have been popularized in science fiction, and are often incorrectly portrayed. They exist nonetheless and can potentially be used for IW.

More than 12,000 computer viruses already exist.[16] Although mostly affecting MS/DOS-operated personal computers, viruses also exist for UNIX machines, "Macs," Windows '95, and other operating systems. There are virus-creation tool kits. There are collections of viruses available for downloading from the Internet, both in executable and source code form. There are computer virus writing tutorials. The future promises even more excitement, as newer generations of Macro viruses come into existence. The future promises local area network-aware viruses, multiplatform viruses, virus mutator, and even viruses in high-level computer languages.[17] As more and more viruses come into existence and gather sophistication, anti-virus tools become less and less capable of dealing with them. As other Internet tools become available, such as Java and ActiveX, viruses certainly will emerge that exploit the new vulnerabilities.[18]

A Reality Check

It is likely that the wholesale adoption of information technologies has only been inevitable. The United States is still the world leader in information technologies and the lure to use those technologies to our benefit is compelling. Science fiction and Hollywood productions glamorize the technology,[19] but other factors have influenced the changes. (The media, for example, probably has contributed to expectations that wars will be like DESERT STORM—executed without excessive cost, fought with a minimum of casualties and collateral damage (at least for our side), accomplished with quickness and efficiency, supported by a number of allies, and undertaken with relatively clear objectives and a well-defined opponent.)

In any conflict likely to confront us in the future, the technology to enable this must be assembled ahead of time, and it must provide sufficiently robust and detailed situational awareness to deal with an enemy that is actually shooting back. Such technology is somewhat expensive, it is fairly complex, it

has numerous vulnerabilities, and it has a number of important consequences:[20]

- ☐ There is a relatively low entry cost for those wishing to participate in IW.
- ☐ The spectrum of potential adversaries increases significantly. It is no longer just a few nations with large militaries. The list of adversaries now includes organized crime, terrorists, etc.
- ☐ Public opinion and perception management become far more important.
- ☐ Information dominance requires large quantities of highly-accurate and high-precision information, as well as the ability to make sense of it all.
- ☐ There are no longer any geographic sanctuaries, as connectivity has rendered distance meaningless.
- ☐ IW mandates careful consideration of the roles of and relationships between law enforcement, the military and intelligence organizations.

Welcome to the exciting new world of IW!

Endnotes

1. Many factors have contributed to that changing nature of warfare. For the United States in 1996, there are several factors which have primarily influenced it. These are that (1) war must not be seen as an excessive drain on resources, (2) it must be clinical (without seemingly needless destruction and loss of life), and (3) it must be lead to a quick U.S. victory. In addition, the U.S. military is increasingly being called upon to accomplish non-traditional missions, such as peacekeeping.

2. It should be noted that the precise number of attacks is not known. The figure 250,000 is based on another estimate that only 1 in 150 attacks is detected and reported.

3. GAO/AIMD-96-84, **Information Security: Computer Attacks at Department of Defense Pose Increasing Risks**, May 1996.

4. As U.S. Army General Sheehan commented in his opening remarks for the information warfare conference 5 (Electronic Civil Defense for the 21st Century—Convergence of the Commercial and the Military Sectors: The Vulnerabilities, Capabilities, and Solutions), the best approach may often be to accomplish objectives while avoiding the "kinetic solution" (the use of military force).

5. The paragraph is based on comments by "experts" on the definition and nature of IW contained in "Information Warfare: Implications for Forging the Tools", a master of science thesis for the Naval Postgraduate School, by USAF Captain Roger D. Thrasher.

6. The specific publications are the electronic magazine ("zine") ***Phrack*** and the quarterly ***2600***. The concept of an organized "computer-underground" is a nebulous one, at best. There are, of course, "hacker" groups and "virus-writing" groups, and they are organized on a local level.

7. Technical solutions to this attack, known as "SYN-flooding" for the part of the IP handshaking it exploits, have been implemented as an add-on. However, the vulnerability still exists.

8. GAO/T-AIMD-96-108, **Information Security: Computer Hacker Information Available on the Internet**, June 5, 1996.

9. GAO/AIMD-96-84, **Information Security: Computer Attacks at Department of Defense Pose Increasing Risks**, May 1996.

10. A conversation with Tom Longstaff, of the Carnegie Mellon University Software Engineering Institute, Computer Emergency Response Team, in September 1996.

11. Timothy L. Thomas, "Russian Views on Information-Based Warfare," ***Airpower Journal***, Special Edition 1996, 26-35. See also Mary C. Fitzgerald, **The New Revolution in Russian Military Affairs**, the Royal United Services Institute for Defence Studies Whitehall Paper Series, 1994.

12. From translation of "Military Forum" column by Zhang Feng and Li Bingyan, "Historical Mission of Soldiers Straddling 21st Century—Roundup of 'Forum for Experts on Meeting Challenge of the World Military Revolution'," in ***Beijing Jiefangjunm,*** 2 January 1996, 2.

13. Ibid.

14. Su Enze's "Military Forum" column, "Logical Concept of Information Warfare," in ***Beijing Jiefangjun***, 11 June 1996, 6.

15. Thoughts extracted from Colonel Alan D. Campen, USAF (Retired), "Information Warfare is Rife with Promise, Peril", by in ***Signal***, November 1993, 19-20.

16. This is only an estimate. There are probably more. The good news is that most of these are variants and that there are only about 720 or so different families." Still fewer of these viruses are typically found "in the wild."

17. "Is the Virus Threat Under Control? An Interview with Vesselin Bontchev, Fred Cohen and Sara Gordon," ***Computer Security Journal***, Volume XII, Number 1, 1996, 57-66.

18. A collection of Increasingly Hostile Applets, a paper obtained from a Web site on the topic of the hostile Java code, in Fall 1996. [Applets are very short Java applications that run on the Internet.]

19. Though it is typically portrayed with significant technical inaccuracies.

20. David Alberts, **The Unintended Consequences of Information Age Technologies**, National Defense University's Institute for National Strategic Studies.

Mr. Anthony is a civilian engineer working at the National Air Intelligence Center at Wright-Patterson Air Force Base, Ohio. He also serves as a major in the USAF Reserve. Mr. Anthony has bachelor and master of science degrees in Computer Engineering from Syracuse University and Wright State University. Readers can reach him at (937) 257-6327, DSN 787-6327, and via E-mail at kda36@naic.wpafb.af.mil.

Information Warfare: Malicious Software and Technology

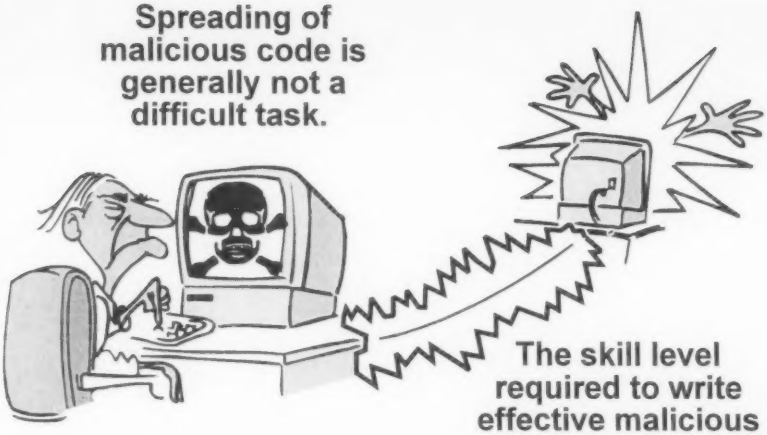
by David L. Potter

Do you care about computer viruses? Would it matter if the information on your computer's hard drives suddenly and without warning disappeared? Would you care if a computer virus got into your service records and showed that you had been killed while on that exercise next weekend or during that deployment next month? Although these situations may seem far-fetched, both of these situations could easily occur by a malicious software code attack.

Most people think of an "attack" as something that usually involves flying metal that could really kill you: bullets, tanks, aircraft, that sort of thing. Most people do not realize that an IW attack could probably do as much damage (or more, depending on who you listen to) as conventional weapon systems, although the initial effects may not be as bloody.

Information, and the systems that the DoD uses to process, change, and distribute that information, have become a vital part of the DoD's infrastructure. You cannot do anything these days without a computer file being changed in some way

Spreading of malicious code is generally not a difficult task.



The skill level required to write effective malicious code has decreased.

somewhere, or having a computer program direct another computer to do something for (or to) you or something you have. All of these computer resources rely on one common element to get the job done—software.

Computer software is contained in almost every weapon system developed by the DoD. The amount of software code that you come into daily contact with could vary from a few lines of code that might be in your digital watch to the several million lines required to control a modern fly-by-wire aircraft. Software controls almost every aspect of everything we do, from the engine in your car to managing your bank account. Although the computer hardware itself is important, it cannot do anything until it is told what to do by software.

Everybody has experienced some occurrence that they thought could be attributed to a "software glitch" such as when the computer on your desk stops working or your car stalls unexpectedly. Who has checked to see if perhaps part of the problem was faulty software code or a computer virus (or other malicious code segment)? Could you tell the difference between faulty code and a virus (or other form of malicious software code)?

Malicious Software

Malicious software has been around in one form or another since the early 1980s when computers first started to appear in the home. Today, malicious software code has probably touched every computer network in existence. When the subject of malicious software code comes up, one generally thinks of its most common manifestation, the computer virus. Most people think of a computer virus as a computer program that causes their computer to crash and delete the information from their computers hard disk. While this is certainly one possible situation, it is not always the only one. Take the Microsoft Word Concept1 Macro Virus (also called the Winword.concept virus); it does not delete any information from your computer, but it does cause "disk full" or "not available" errors or it places the document in a directory that you would not normally use, making it difficult to find later.

There are somewhere between 9,000 and 12,000 computer viruses in existence today, depending on whose numbers you use. Viruses, though, are only one possible type of malicious code. Malicious codes include—

- ☐ Nine different types of viruses: Bootstrap Sector, File Infector, Memory Resident, Non-Memory Resident, Multi-Partite, Stealth, Polymorphic, Network-Specific, and Bounty Hunter viruses.
- ☐ Worms, programs which can move independently from computer to computer via a network. They generally aim at increasing the time required to perform a particular task, thereby slowing down the network or system on which it is running.
- ☐ Trojan Horses, programs which say they do something useful, but contain a section of code that can be destructive or have other hidden capabilities.

Although the term "virus" is used to refer to malicious software code in general, the terms "virus," "worms," and "Trojan Horse" are becoming less meaningful. Because malicious code can be developed that would perform a particular function (and possibly perform this function on a particular computer or computer network), the typical definition of the code segments will not adequately identify the code segment or capability.

Propagation

Can malicious software operate on a computer running UNIX as well as a computer using MS-DOS? Quite possibly the answer is yes. Although some types of computers operate using different processors (e.g., Motorola versus Intel), the operating system (including UNIX, MS-DOS, MacOS, OS/2) is what controls how the hardware really works. Although DoD may have some nonstandard computers that perform dedicated functions without an interface to other computers (one example of this is the computers that control a fly-by-wire aircraft), most computer systems are procured as off-the-shelf commercially available items. The commercial market has dictated that some software operate on multiple platforms; as an example, DOS applications can run on UNIX platforms using the X-Windows environment. Although this is not a guarantee that a virus will be capable of infecting both operating systems, it is an indication of compatibility.

The commercial market has dictated a commonality of hardware that allows users with different requirements to use interchangeable systems; computer hard-drive units are one of the best examples of this. Small Computer System Interface (SCSI)-based computer drives can be used in any computer. It is this commonality that creates the greatest opportunity for the successful

transmission of a malicious code segment. Because the hardware is standard, the software that controls the hardware and serves as the interface between the hardware and the application (i.e., drivers) relies on the same set of commands to access the hardware. Because malicious code (and viruses in particular) generally executes a specific command set (such as writing "Ø"s to the boot sector of the drive as one example), writing a code segment that has capabilities against several operating systems is quite possible.

As malicious code is developed for specific applications, it is possible that one could be developed that would initially infect one platform (and operating system) and then migrate to another platform or application. The ability to do this will depend to a large degree on the skill of the virus writer, and the desired effect of the virus (or code segment) on its target. It is quite possible to develop a virus that would be capable of operation in several OS environments, even though the number of existing viruses for DOS systems is far greater than any other OS.

Spreading of malicious code is generally not a difficult task. In most cases, a commonly used file is infected (game programs are a particularly good example, but are by no means the only type of "carrier" file); the popularity of the particular file causes it to generally be spread to many other users. As the program is executed, other files on the computers hard drive are infected. Other documented means of dissemination have included shrink-wrapped software obtained from a major software manufacturer; there have been several cases of this, and they have been traced back to infected files in the compiler used in the development of the original software.

The global connectivity of computers and computer networks has helped to create an environment conducive to the transmission of malicious software. Files are routinely transferred from one location to another within organizations. Searches of the Internet are conducted to locate particular files or programs—programs used for entertainment, to enhance systems' performance, or any one of a number of other uses. Unfortunately, most organizations do not make effective use of anti-viral software to screen incoming files for the presence of malicious code, thereby proliferating the virus.

Writing Malicious Code

The skill level required to write effective malicious code has decreased in the past few years. Writers of malicious code now have several tools available to assist in the writing of code—

- ☐ A standard Windows-like graphical user-interface.
- ☐ Pull-down menus.
- ☐ Features allowing for the incorporation of capabilities for the code to change itself, making detection much more difficult.
- ☐ Most of these programs are readily available on the Internet.

Virus writing "organizations" exist on the Internet; they routinely exchange ideas, technical information, code segments, and methods of infection. Participants generally have an intimate knowledge of the various computer operating systems, anti-viral software characteristics, and a desire to write efficient code. The groups do collect and study viruses and other code segments, the goal being to make them more efficient and less likely to be detected by anti-viral software.

With one exception, there are no confirmed cases where malicious code was written to accomplish a specific task (the goal of destroying data on a hard drive is not considered a specific task in this context); this one exception was the Word1.concept virus. This "virus" was written to demonstrate that a malicious code segment could be propagated without infecting a .COM or .EXE file.

Code Capabilities

Most current malicious software takes the form of computer viruses. The most common features of viruses are to display a message indicating that the system has been infected, and then overwrite portions of the hard drive (destroying data in the process). Do malicious codes perform other tasks? Yes, although there have not been many documented instances of this occurring. Take for instance a targeted attack, such as one that would change your status to deceased. A code segment could be written that would spread, without activating, until it reached a particular IP address. Once the desired address had been infected, the virus would activate and search for fields in a database of personnel information. When the appropriate field had been determined, the coding would be changed to indicate that the individual was now deceased (for those who think correcting this problem would be easy, think about how the government bureaucracy works). This particular kind of attack would require a significant amount of prior knowledge about the targeted system; this information would have to be stored in the virus itself, probably making the virus itself too large and cumbersome to reach its destination undetected.

What malicious code developments are likely to occur? Code segments themselves will likely be smaller and more efficient than they are currently. It is also probable that code segments will be written that will target either a particular system, capability, or operating feature. Depending on the motivation of the particular writer, specific systems could be targeted, possibly by using keywords or some prior knowledge of the target system. It is also likely that nondestructive code segments will be written that would perform functions such as system monitoring, analysis of system vulnerabilities, or information gathering. Such code segments could report back to a central point, using the computer's own network capabilities to do so. Because this type of code would not operate like current virus code, current anti-viral software may not be capable of detecting it. Detection would be possible, but would require some knowledge of the vulnerabilities of the weapons or information systems, with a code segment written into the systems'

operating software—something that will require recognition of the threat by the material developers.

Impact of Technology

Technology is progressing at a significant rate, both in hardware and software. New software developments in the commercial sector have taken into account the threats posed by malicious software code. Windows '95 is one example; it was designed with security features that would make its vulnerability to malicious code difficult. It did this by structuring the operating system so that only trusted code segments could perform critical system operations. As good as the effort was though, a virus capable of attacking Windows '95 does exist. This is a situation that will persist for quite some time. The motivation of the malicious code writer is basically the challenge of developing something thought to be impossible. As long as this motivation exists, there will always be a threat; it would be cost-prohibitive to design software completely invulnerable to attack.

The other factor that will play a significant role in this area is the advancements in hardware. Hardware developments are occurring in which multiple operating states exist (the Pentium processor is one example). Malicious code will likely be written that will capitalize on these background operating states; because current anti-viral software searches for specific virus operating characteristics, working in background states could offer the advantage of longer operation without detection. Because the development of anti-viral software is currently reactive rather than proactive, the development of different effective countermeasures against this particular type of code will depend on how long it takes to detect it.

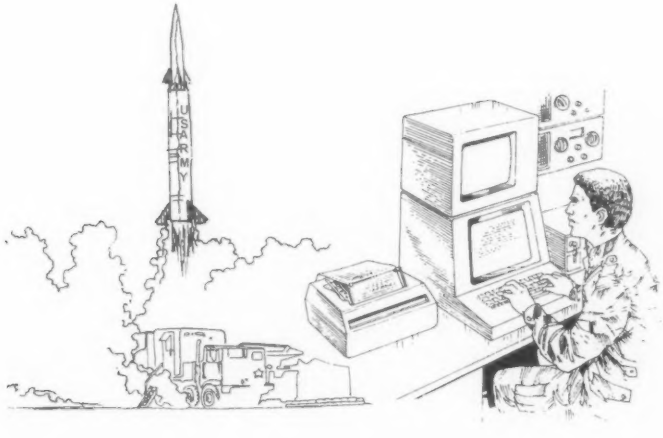
One final consideration is that current anti-viral software is targeted against **viruses**, and not other forms of malicious code. It is important to realize that other forms of malicious code could be far more dangerous to operations than just the destruction of data caused by viruses—impacted operations could include tactical, strategic, and sustaining base, but would most likely originate against the private sector (targeted areas would likely include financial and industrial areas). The reason for this is that the potential gain could be far greater in these areas, at least initially. Targeting these areas could also allow for the refinement of techniques that could then possibly be used against military targets.

Conclusion

Not all computer problems result from malicious software. Operations are more likely to be adversely impacted by defective code than malicious code (bear in mind that software testing generally does not look for defective code, only proper operation of intended functions). Awareness of the threats is important; educating systems users about the threat is the key to maintaining awareness and vigilance. Use of the latest anti-viral software is critical to ensuring that this threat does not adversely impact operations. Adherence to proper computer security programs and goals are essential to ensuring that threats are identified before they can become operational problems.

Mr. Potter is an Electrical Engineer currently working in the Acquisition and Technology Support Division of the Directorate for Intelligence and Information Security, U.S. Army Communications Electronics Command. He is a 1983 graduate of California State University with a bachelor of science degree in Mechanical Engineering. Readers can reach him at (908) 532-5873, DSN 992-5873, or via E-mail at Potterd@doim6.monmouth.army.mil.

Non-Nuclear EMP: Automating the Military May Prove a Real Threat



by Major Scot W. Merkle

How is this for a grand scenario?...One that would make an airborne assault with combat equipment, followed by a twenty-five-mile forced march sound enticing. You are the operations officer (S3) of your battalion and tomorrow you are to present your one-hundred-plus slide quarterly training brief (QTB) presentation, but for some unknown reason, all of the automation equipment on post is down. You hurry home to print it on your own personal computer (PC), but your system is also down (and you just spent the whole weekend with that

new income tax software working on your return).

You wonder...How could such a catastrophe occur? What could cause this to happen? Then you remember the movie that you saw this past weekend. About ruthless forces threatening to use a weapon capable of destroying the computer chips and memories upon which our lives depend. But one man stood in their way: "Bond... James Bond!"

Hollywood shenanigans? Implausible? Science fiction? The answers are yes, no, and maybe. The 007 saga "Goldeneye" is about attempts to prevent the neophyte, but dangerous, Russian Mafia from using an orbiting space weapon (called Goldeneye), which can blast uncooperative nations with pulses of energy, harmless to people but devastating to electronic devices and their components. Airplanes would fall from the skies, nuclear-power plants would race out of control, financial records would be erased, and your one-hundred-plus QTB slide presentation would be lost.

Could this actually happen? The fact is, that today, there is technology available that could do just that. Fortunately, international treaties governing the use of outer space and the availability of the simpler, non-nuclear-pulse weapons make the specifics from the "Goldeneye" scenario improbable. Then again, the military has earned a reputation for falsely labeling as fiction advanced weapons and units already within its arsenals; remember the Pentagon's embarrassment when surprisingly accurate models of its supposedly super-secret stealth-fighter aircraft began appearing at your local toy store?

Real EMP Weapons

In reality, the existence of Goldeneye-like pulse weapons first became a fact in the early 1960s. While testing hydrogen bombs in outer space, hundreds of miles above the planet, American and Soviet scientists discovered that each atomic blast created a pulse of electromagnetic energy similar to conventional radio-made microwaves, but with energy so great that they erased magnetic memories and melted the microscopic junctions in transistors on the Earth below. These were veritable tidal waves of energy, sufficient to cripple sensitive microelectronics but too weak to be seen, heard, or felt by human beings.[1]

During one U.S. test, in July 1962, a hydrogen bomb was detonated approximately 650 miles in space, roughly where today's space shuttles orbit. Simultaneously, 2100 miles to the northeast, street lights went dark and burglar alarms began ringing on the Hawaiian islands. The reason was an electromagnetic pulse (EMP) produced by the blast.[2]

Due to this reaction, in 1963 the United States and the Soviet Union signed the Atmospheric Test Ban Treaty to counter the considerable threat posed by EMPs. Since then, that threat has grown at a fantastic rate, fueled by the rapid progress made in compacting ever more EMP-sensitive transistors onto the computer chips upon which modern electronics rely.[3] Can you imagine your neighbor being able to go down to the local radio parts store, buy a hand-held EMP weapon, and use it to wipe out your household electronics? All because he is angry at you.

According to a declassified U.S. military report, the explosion of a bomb about one megaton in size (the exact size remains classified) eight hundred miles over Omaha, Nebraska, would shower the continental United States, southern Canada, and northern Mexico with an EMP capable of disabling virtually every computerized circuit in its path. Edward Teller, the father of the hydrogen bomb, succinctly described the damaging consequences of such an EMP attack in 1982, when he wrote in an obscure engineering journal—

> *Today there is almost universal dependence on electronic computers. They are used by first-graders as well as research engineers. Industry, communications, financial records, are all at stake here. In the event of heavy EMP radiation, I suspect it would be easier to enumerate the apparatus that would continue to function than the apparatus that would stop.*[4]

Are you now beginning to reconsider that purchase of the latest superhot mini-tower PC? Relax. It is unlikely that a nuclear blast will occur in space any time soon. The Outer-Space Treaty of 1967, since ratified by the members of the United Nations, explicitly states that treaty partners not place any objects carrying nuclear weapons in Earth's orbit—great idea, in principle. The trouble is, the treaty does not oblige any nation to allow others to inspect the cargo they send into space.[5] So, if Iraq obtained nuclear weapons and was capable of launching them into a space orbit around the Earth for detonation over the United States (in revenge of Operation DESERT STORM), you could kiss your fancy E-mail system goodbye.

The Non-Nuclear EMP Threat

So, to this extent, the plot of "Goldeneye" is plausible. Any of several nations with nuclear weapons and the capacity to launch them into space—including the United States, Russia, China, and even Israel—could conceivably pulse us back to, shall we say, a simpler time when operations orders were done orally with a sandtable, instead of with the high-speed graphics and charts that turn into an encyclopedia that few people care to read. Even more unsettling, however, is the fact that the U.S. Defense Technology Plan confirms that development of advanced EMP weapons continues to this day, and not just by the Americans. According to a report drafted by conservative members of the French National Assembly in 1992, EMP weapons testing was a recommended goal during France's 1995 underground nuclear tests.[6]

Some really scary parts of the EMP story did not make it into James Bond's latest adventure. Weapons designers specializing in high-energy physics can now create electromagnetic pulses without going into outer space. One approach involves harnessing the force of a

conventional explosion. Others are simply just modifications of radar, which bounces pulses of energy off aircraft in flight, vehicles on the ground, and other objects.[7] Crank up the power and you have an EMP weapon, ready to point at the computers of your favorite enemy.

This knowledge has set off a new arms race. Whether fitted into cruise missiles or parked at the side of the road in a van, non-nuclear EMP weapons have the potential to devastate the electronic systems of areas as large as a city or as small as a selected building, all without being seen, heard, or felt by a single soul.[8] It is a dream come true for any and all terrorists, to include Saddam Hussein himself!

Sound far-fetched? It did not in 1993 to the owners of automobiles parked about 300 meters from a U.S. Defense Contractor's EMP generator test site at Eglin Air Force Base in Florida. Their alternators and electronic engine controls were accidentally fried by a pulse during classified field trials.[9]

Specific Threat to the Military

So what is the non-nuclear EMP threat to our military today? It is, put simply, that while we are quite enamored of our technological progress, we would do well to ensure that basic infantry skills, those things that have enabled America to have the greatest army in the world, are not forgotten. It can be readily observed that the United States is devoting a significant amount of time, energy, and hard working taxpayer dollars to "push the technology envelope" to prepare for the Force XXI battlefield.

The Army will equip tomorrow's infantry soldier with a totally integrated fighting system that takes full advantage of technological advances. Their fighting load modules include vests with removable ammunition pouches enabling them to carry the soldier radio, battlefield computer, global positioning system (GPS), and required antennas. One burst of EMP will render this equipment inoperable, rendering the 21st century land warrior ineffective on the Force XXI battlespace. He will still be able to fight, but without his wondrous gadgets and gizmos.

Conclusion

Therefore, it seems to me that while developing and implementing technologies and strategies for the Force XXI battlespace, we also need to emphasize force modernization in developing technologies and strategies to counter the EMP threat. It is even more important that our junior leaders and soldiers become and remain exceptionally proficient in basic skills of land navigation, small unit tactics, and sandtable operations and operations orders. I would not discard that Ranger handbook just yet. At the battalion level, I recommend that the battalion intelligence officer keep those grease pencils, templates, and manual weather forecasting equipment handy because the Joint Surveillance and Target Attack Radar System, All-Source Analysis System, and most other "high tech" intelligence connectivity systems will not be working.

In sum, while I advocate taking full advantage of any and all technologies that will enhance our ability to fight and win America's battles, we must not lose sight of one essential fact. Gadgets and gizmos do not take and hold terrain, nor do they fight and win on the battlefield—well-trained soldiers do! Non-nuclear EMP has the potential to reduce the battlefield equation to very simple terms. I submit that in this scenario, "back to basics" becomes more than a simple cliché. Stripped of the technology, the soldier who is well versed in basic soldiering skills will be victorious.

One thing is certain: in case of an EMP attack, don't bother calling James Bond. Your telephone won't be working.

Endnotes

1. Harry Gefen, "Mind & Matter", ***The Globe and Mail***, (9 December 1995), D-8.
2. Ibid, D-8.
3. Ibid, D-8.
4. Ibid, D-8.
5. Ibid, D-8.
6. Ibid, D-8.
7. Ibid, D-8.
8. Ibid, D-8.
9. Ibid, D-8.

Major Merkle is a student assigned to the Air Command and General Staff College, Maxwell Air Force Base, Montgomery, Alabama. He has served in numerous intelligence positions such as Assistant S2 and S5, 1st Ranger Battalion; Assistant S2 and Special Security Officer, 75th Ranger Regiment; and S2, 3d Ranger Battalion. Major Merkle is a graduate of Glassboro State College in New Jersey and holds a bachelor of arts degree in Geography. Readers can contact him via E-mail at scmerkle@max1.au. af.mil.

MI Corps Hall of Fame Nominations

The Office of the Chief of Military Intelligence (OCMI) accepts nominations throughout the year for the MI Hall of Fame. Anyone can nominate an individual for induction into the MI Hall of Fame. Commissioned officers, warrant officers, enlisted soldiers, or civilians who have served in a U.S. Army intelligence unit or in an intelligence position in the U.S. Army are eligible for nomination.

A nominee must have made a significant contribution to MI which reflects favorably on the MI Corps. In certain isolated instances (particularly in the case of junior soldiers), the nomination may be based on heroic actions rather than other documented contributions.

Nominees cannot be employed by the U.S. Government in any capacity at the time of their nomination. Individuals cannot be self-nominated. An annual Hall of Fame Board convenes to review nominations and make recommendations to the Chief of MI who is the final approving authority for inductions into the Hall of Fame.

The OCMI provides information on nomination procedures. If you wish to nominate someone, contact OCMI, U.S. Army Intelligence Center and Fort Huachuca, ATTN: ATZS-MI (Hall of Fame), Fort Huachuca, AZ 85613-6000; or call commercial (520) 533-1181, DSN 821-1181, or via E-mail at chamberj%hua1 @huachuca-emh11.army.mil.

The Internet: Resource or Quagmire ??

by Chief Warrant Officer Four Alan D. Tompkins, USAR

Is the Internet a useful and productive resource for an intelligence analyst or is it merely an interesting world of time wasters and diversions? News stories, magazine articles and conversations about the Internet bombard us on a daily basis. Friends tell us about the new version of a Web browser they are using. They pass on interesting uniform resource locator (URL) addressses. Students "surf the net" to find information needed for school reports. Exciting as all that may seem, should a professional intelligence analyst working in an environment marked by budget constraints and limited resources devote time and energy to exploring the Internet?

As often happens, the answer to that question contains some good news and some bad news. Beyond that, effective use of the Internet is not a simple matter. As is often said, "the devil is in the details."

The Good News

The Internet provides access to a huge and varied collection of open source information (OSI). OSI contributes to the analysis process by providing an understanding of the broad framework of a situation. Dr. Joseph Nye's jigsaw puzzle analogy explains the relationship between OSI and the classified disciplines. In paraphrase, he has noted that—

Open source intelligence provides the outer pieces of the jigsaw puzzle, without which we can neither begin or complete the puzzle. But they are not sufficient of themselves. The precious inner pieces of the puzzle, often the most difficult and most expensive to obtain, come from the traditional intelligence disciplines. Open source intelligence is the critical foundation for the all-source intelligence product, but it cannot ever replace the totality of the all-source effort.[1]

The Internet is a network of networks of computers, which in the last two years, has exploded in size. Estimating the actual number of people and organizations connected to the Internet is a difficult task but probably at least 30 million individuals and 40,000 networks are connected, and these numbers are expanding rapidly. Certainly, some of the opinions, observations, and publications of a group this size can be both interesting and useful sources of OSI.

The quantity of data available on the Internet is enormous. One estimate is that the total content is from 2 to 10 terabytes. A terabyte is a million megabytes, or one million, million characters. By comparison, a typical public library with 300,000 books has about 3 terabytes of data.[2]

The contents of the Internet range from newspaper and journal archives and scholarly papers to messages exchanged between rock star fans. Many companies, governments, and organizations publish information on the Internet. Thousands of newsgroups organized by topic contain messages and discussions about almost every aspect of the human condition; from pickle recipes to heated discussions of cultural and political issues. Because publishing information on the Internet is inexpensive when compared with traditional print methods, organizations, military units, and governments increasingly use the Internet to provide information to their customers, members and citizens.

In summary, the Internet can be a useful, readily available and inexpensive resource that can provide a significant part of the total information required to produce all-source intelligence products. For areas and topics not normally targetted by classified means of collection, open sources in general and the Internet in particular can provide a broad, continually updated view to the all-source analyst.

The Bad News

It is important to note, however, that the Internet is just one source of OSI. Thousands of databases are available from commercial providers such as LEXIS/NEXIS, Reuters, and Dialog. These commercial sources are often better organized and indexed than material available on the Internet, but they are also more expensive.

Searching for information on the Internet requires skill, persistence, and powerful searching tools

Writing in 1993, Admiral William Studeman, then Deputy Director of Central Intelligence stated—

We have identified some 8,000 commercial databases—and the vast majority have potential intelligence value. The number of worldwide periodicals has grown from 70,000 in 1972 to 116,000 last year. The explosion of open source information is most apparent in the Commonwealth of Independent States [the former Soviet Union], where today, there are some 1,700 newspapers that were not published three years ago.[3]

It is also important to understand that despite rapid growth in the availability of OSI in digital, online format, probably less than 10 percent of all OSI is available in that format. The remainder exists in printed, hard-copy formats: books, newspapers, journals and reports.

As mentioned above, the total estimated content of the Internet is roughly equivalent to two or three typical public libraries each containing 300,000 volumes. However, the largest OSI repository in the world is the U.S. Library of Congress which has more than 107 million books, newspapers, journals, microforms, other special format materials in 470 languages, and approximately 200,000 current periodicals, 80,000 of which are in foreign languages.

Unlike a traditional library, the contents of the Internet are constantly changing. Sites appear and disappear and the contents of individual sites can change daily. A University of Colorado study published in 1992 when content on the Internet was far less dynamic, found that the average life of a document on the network was only 44 days. Currently, document life is probably much shorter.[4]

Also, unlike libraries or commercial databases, the Internet is not maintained by professional Librarians. There is no standard subject list like the standard Library of Congress subject headings. Different terms describe similar topics on different sites. Searching for information on the Internet requires skill, persistence, and powerful searching tools.[5]

The challenge in making effective use of the Internet is finding the needle in the haystack. OSI on the Internet is so diverse, scattered, and voluminous that it can easily overwhelm the analyst. Effective use of OSI demands skilled analysts following clearly defined search plans and using increasingly sophisticated computerized tools.

Small wonder that a group of senior Marine Corps officers, led by the Assistant Commandant of the Corps, visited the New York Stock Exchange recently to learn how brokers absorb, process and transmit the vast quantities of perishable information that are the lifeblood of the financial markets.[6]

So, the bad news about the Internet is that it contains only a portion of the total available OSI resources, its contents change very rapidly, and it is not very well organized or indexed.

The Details

Searching the Internet can easily be like a trip to the shopping mall to buy a pair of shoelaces. You start out by knowing what you want, but there are distractions along the way. First, you smell pizza, so you buy a slice. Then, there are some interesting books on display in the book store, so you browse for a while. After that, you buy some frozen yogurt and a T-shirt with a catchy phrase on the back. After an hour and a half, you hurry back to work with a slightly upset stomach, a few little packages, and no shoelaces.

The Internet has become something of an information Nirvana, an enormous, multicultural library that is open all day, every day, to ordinary computer users. Taking advantage of this amazing institution, however, requires some savvy. Users need to know not only how to get in the door but also which aisle to choose from in a maze of thousands that will take them to the document they seek.

Clearly defined and managed collection plans are essential. Also, a stable, well-understood set of searching, storage and retrieval tools is necessary to ensure high analyst productivity. Because of the high level of activity and growth on the Internet, new tools are released on almost a an daily basis. It is tempting to try each new program that becomes available. If the analyst's tools change continuously, more effort will be spent in understanding tools than in collecting information.

Major Mats Bjoere of the Swedish Army has published an excellent paper that outlines the main elements of a well managed and organized OSI collection effort.[7] It contains a number of lessons learned in running an OSI operation.

Conclusion

The Internet does contain information useful to the all-source analyst. It can provide the critical outer pieces of the jigsaw puzzle described by Dr. Nye. However, it is only one part of the vast world of OSI and it can only be exploited successfully and efficiently by well-trained analysts using a proven tool set following clearly defined collection plans.

Endnotes

1. Dr. Joseph Nye, the Chairman of the National Intelligence Council, speaking to members of the Security Affairs Support Association at Fort Meade, Maryland, on 24 April 1993.

2. Rajiv Chandrasekaran, "In California, Creating a Web of the Past," ***The Washington Post***, 22 September 1996, H1.

3. Admiral William O. Studeman, "Teaching the Giant to Dance: Contradictions and Opportunities in Open Source Information within the Intelligence Community," ***American Intelligence Journal***, Spring/Summer 1993, 19.

4. Ibid, H14.

5. Ed Krol, **The Whole Internet User's Guide & Catalog**, (Canada:O'Reilly & Associates, Inc.), Second Edition, 1994, 235.

6. Eliot A. Cohen, "A Revolution in Warfare," ***Foreign Affairs***, March/April 1996, 43.

7. Mats Bjoere, Major, **Six Years of OSI**, http://www.eajardines.com/mats2.html.

Mr. Tompkins is currently a consultant providing advice on training and custom software development. He is also a reservist with the 434th Military Intelligence Detachment (Strategic) in New Haven, Connecticut. Mr. Tompkins has taught software design methodology at Beijing University and worked as a systems engineer with International Business Machines. He has a bachelor of arts degree in Russian Studies from Yale College and a master of science degree in Computer Science from Rensselaer Polytechnic Institute. Readers can contact him at 76314.2052@ compuserve.com or (802) 862-2240.

Owning the Weather

Weather Support to Force XXI

by Richard J. Szymber

Critical Army thrusts such as Digitize the Battlefield, Own the Night and Own the Weather are vital to winning the information war....Owning the Weather is one of the force multipliers that will ensure Land Force Dominance by giving the warfighter the information he needs to fight under all weather conditions...We will Own the Night and the Weather so we can support day, night, all weather operations.

—General Jimmy Ross, Feb. 1994

The history and lessons of weather and war are enduring. Historically, weather has decisively impacted battlefield success, and warfighters prepared to exploit the effects of weather and terrain will benefit in any battle. In the timeless words of Sun Tzu from **The Art Of War** written over 2000 years ago: "Know the enemy, know yourself; your victory will never be endangered. Know the ground, know the weather; your victory will then be total." Instead of reacting to the weather with a cope-and-avoid mentality, Force XXI warriors will anticipate and exploit it.

Owning the Weather

"Owning the Weather" is about understanding, anticipating, and exploiting the impacts of weather on both friendly and threat capabilities to gain a warfighting edge over enemy forces. Owning the Weather (OTW) will soon provide Force XXI an effective "all-weather" mission capability by giving the warfighter the information he needs to fight and operate smart weapons and munitions in all weather conditions. It will enable commanders and soldiers to fully exploit tactics that maximize the weather-related advantages our forces have over the threat.

OTW is the use of advance knowledge of battlefield environmental conditions and their effects on friendly and threat soldiers, systems, operations and tactics in order to gain a decisive advantage over opponents. It involves exploiting and improving the weather-derived technological advantages of our battlefield operating systems (BOS) over hostile systems, making adverse weather a force multiplier.

The OTW operational strategy for battlefield weather exploitation involves three basic steps. First, a variety of battlefield sensing systems must observe and collect, in real time, the actual meteorological conditions for the entire area of operations, including critical, data-denied target areas. Then this information must be processed, analyzed, and disseminated rapidly to the user. The input of the observational data into models is essential for forecasting atmospheric conditions and their effects. The final step concerns the combat application of the observations, forecasts and effects, and their transformation into usable battlefield weather-visualization products. These include weather analysis displays for the intelligence preparation of the battlefield (IPB) and automated weather-effects decision aids.

Weather Architecture

Weather conditions must be observed before they can be forecast and ultimately converted into weather intelligence. No single sensing system can supply all the diverse observations required. Therefore, a variety of complementary space-based, airborne, and ground-based sensing systems will provide observations at the required accuracies, resolutions, and coverages. The data collected from every available source is validated and combined with appropriate models to build a complete, detailed, and accurate horizontal and vertical picture of the atmosphere and weather over the full extent of the battlefield.

The OTW long-range data collection concept for the time period from 2005 through 2015 appears graphically in Figure 1. The Integrated Meteorological System (IMETS) serves as the integration (fusion) point for the weather data from all sources:

- ☐ National Polar-Orbiting Operational Environmental Satellite System (NPOESS) and the

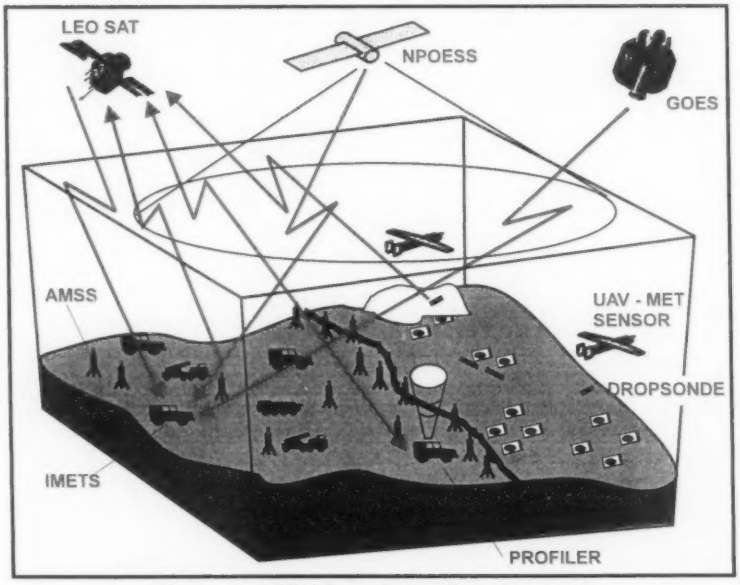


Figure 1. OTW Data Collection Concept.

U.S. and foreign Geostationary Operational Environmental Satellite (GOES) transmit real-time space observations.

- ☐ Automatic Meteorological Sensor Systems (AMSSs), and/or Improved Remotely Monitored Battlefield Sensor System (IREMBASS) with meteorological sensors placed at key locations will send real-time surface weather and ground-state data over area communications.
- ☐ The Field Artillery Meteorological Section's atmospheric profiler and Computer-Assisted Artillery Meteorology (CAAM) model will transmit upper-air weather profiles via Mobile Subscriber Equipment (MSE).
- ☐ Unmanned aerial vehicle (UAV) target area weather observations will reach the IMETS in near-real time through the UAV tactical control station.

IMETS is a tactical, automated, mobile, weather-data system designed to provide timely weather- and environmental-effects forecasts and decision-aid information to appropriate command elements. For lower echelons without direct weather support (for example, brigade and below), software on command and control (C^2) systems will allow them to request weather information from a division IMETS and produce weather effects decision aids, using weather data passed through the Army Battle Command System (ABCS). IMETS capabilities will include—

- ☐ Satellite, tactical radio and MSE communications.
- ☐ A battlescale forecast model for high-resolution local weather prediction.
- ☐ Automated decision aids for weather effects.
- ☐ Weather-forecasting decision aids, and tools.

OTW will provide a digitized, real-time, dynamic shared picture of the battlespace weather, and its effects for IPB, mission planning and rehearsal, situational awareness, synchronized battle management, and advanced decision and execution support. The IMETS will collect data from various sources and disseminate timely battlescale weather information to multiple command elements via the ABCS and the All-Source Analysis System (ASAS). Tactical decision aids (TDAs) and displays resident on computers of the BOSs will use this information to provide warfighters with real-time and predicted environmental effects on operations. The capabilities will include user-tailored weather support TDAs, critical-value databases containing information on the weather sensitivities of friendly and threat systems, and automated comparison and assessment of weather effects on both friendly and threat capabilities.

Commanders and their planners must consider weather effects in all phases of operations, so that the best course of action (COA) can be chosen for each mission. Weather support TDAs allow commanders to manipulate and present real-time and predicted weather information, showing its effects on terrain and combat systems. They also allow planners to wargame COAs in anticipation of changes in the weather. The Integrated Weather Effects Decision Aid (IWEDA) is a sophisticated expert system that provides these capabilities. It automatically identifies unfavorable, marginal, and favorable weather-effects information based on the operating limitations of friendly and threat weapon systems. IWEDA is tailorable to specific tactical operations and missions, providing color-coded time-dependent assessments of weather effects on mission and equipment performance.

The commander and planners require weather information before deployment, enroute, and in the area of operations to support force projection operations. A small, lightweight, soldier-packable first-in weather operations system, along with split-based capabilities, will provide the ability to move quickly with the early-entry forces. (See Figure 2.) Commanders and their staffs will be able to "pull" in weather intelligence tactically tailored in the required format when needed (including while on the move). The Air Force Global Weather Center (AFGWC) will provide

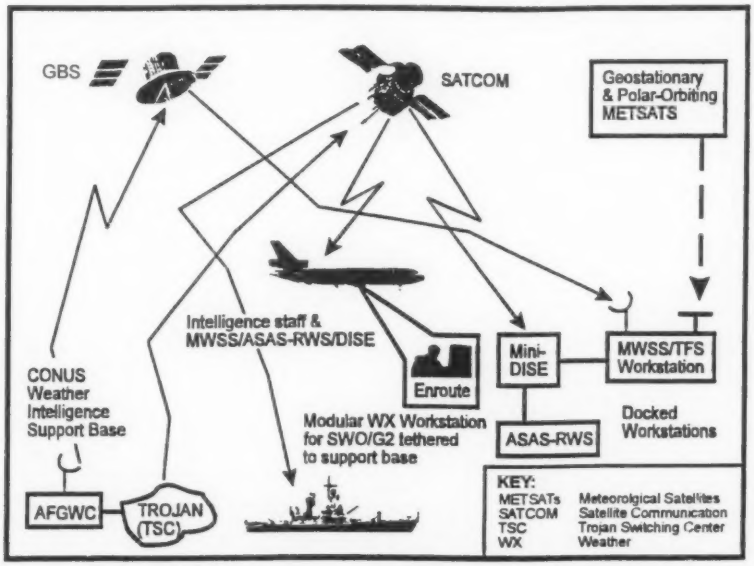


Figure 2. Weather Intelligence Split-Based Force Projection Ops.

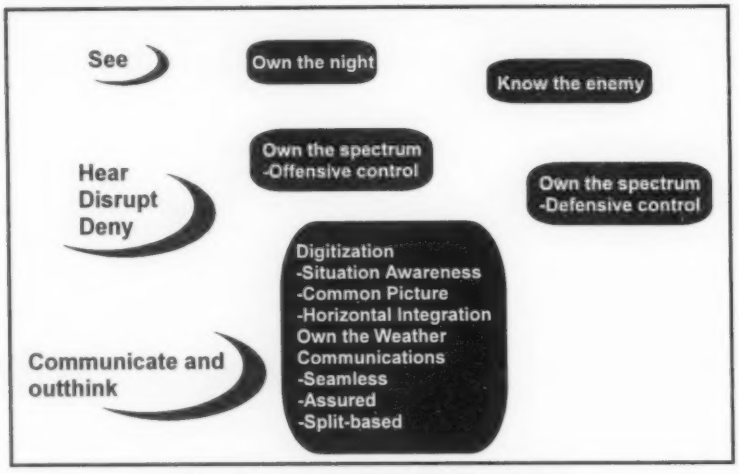


Figure 3. Information War Functions.

support to split-based operations. The AFGWC will work through the Global Broadcast Service and the TROJAN Special Purpose Integrated Remote Intelligence Terminal II, via the Tactical Forecast System (TFS) in conjunction with the Deployable Intelligence Support Element (DISE). Together with the IMETS, the first-in weather capability will provide units a Manportable Weather Support System (MWSS) package, able to truly support the level and urgency of any contingency.

Military Intelligence Applications

Weather is one of the essential elements of combat intelligence. The interaction of weather, terrain, and the enemy forms the basis for the IPB process. The commander's primary tool for presenting and analyzing the effects of weather and terrain is IPB. In the context of IPB, weather intelligence is the process of converting weather observations and forecasts into weather-effects information portraying the impacts of weather on both our operations, troops, and equipment and that of the enemy. In the IPB process, weather analysis includes—

- ☐ Comparing observed and forecast conditions against critical weather-effects threshold values and identifying limitations on operations.
- ☐ Evaluating the effects of precipitation on mobility and countermobility, on trafficability, and on deep-attack weapons and operations.
- ☐ Comparing friendly and threat capabilities in varied adverse weather conditions.

OTW automated IPB weather analysis products will provide the commander and his staff with the capacity to immediately assess how current and future weather conditions affect enemy activities and events, and both the friendly and threat force's ability to fight. This automated capability will enable the revision of IPB products such as the situation template in near real-time using the most current information available. All of this will enhance our ability to see the battlefield in four-dimensional time and space, and the commander's skill in determining the enemy's expected COA as well as his own.

Some critical capabilities for Intelligence XXI that OTW will provide include—

- ☐ Reliable target-area weather data for precision-strike targeting accuracy and battle damage assessment.
- ☐ All-source fusion of environmental information for modeling current and future weather effects on terrain and combat operations.
- ☐ Reliable communications for weather-intelligence dissemination.
- ☐ A scalable, dynamic view of battlespace weather: simulation and visualization of battlefield weather effects for real-time and predicted shared situational awareness.
- ☐ Mobility comparable to that of the supported force and an ability to maintain the operational tempo through enhanced knowledge and understanding of weather effects.

Information Operations

The force multipliers that are embodied within information war can be defined as **see** the enemy, **hear** and locate the enemy's C^2 structure, **disrupt** the C^2 structure by physical destruction, **deny** hostile C^2 by jamming, and **communicate** and **out-think** the enemy using a robust C^2 system and assured seamless communications. Many capabilities support these battlefield functions including those listed in Figure 3.

Situational awareness and the relevant common picture enable commanders to perceive changes in the environment and then act upon those changes to produce a desirable end state. Battlefield visualization of weather, and its effects, is an essential element of battle command, and is necessary for out-thinking the enemy and gaining information dominance. OTW provides the capability to anticipate the differential impacts of weather on friendly and threat capabilities allowing commanders to exploit windows of opportunity created by the weather.

The OTW process for knowing, applying, and integrating the weather encompasses—

- ☐ Battlespace sensing and data collection.
- ☐ Processing, analysis, forecasting, and dissemination.

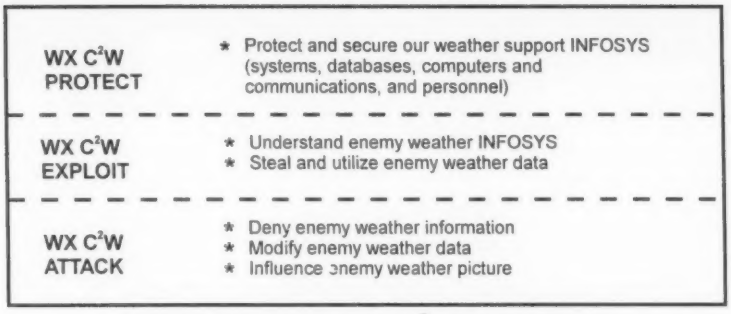

WX C²W PROTECT
* Protect and secure our weather support INFOSYS (systems, databases, computers and communications, and personnel)
WX C²W EXPLOIT
* Understand enemy weather INFOSYS
* Steal and utilize enemy weather data
WX C²W ATTACK
* Deny enemy weather information
* Modify enemy weather data
* Influence enemy weather picture

Figure 4. Weather (WX) C^2W Components.

- ☐ Battlefield visualization and decision aids.
- ☐ Combat weather exploitation and information operations (IO).

The purpose of OTW IO is to guarantee and maximize our ability to exploit the weather to our advantage while simultaneously denying the enemy's ability to use or manipulate the weather to his advantage. It is crucial to deny the enemy access to meteorological satellite information in order to maximize our advantage. Improved weather information and IO, combined with knowledge of the limitations of weather on warfighting capabilities, is a powerful IW weapon.

The thrust of OTW IO has three parts. (See Figure 4.) These objectives are accomplished by protecting our weather information system (INFOSYS) and attacking the enemy's INFOSYS, through weather C^2W-protect and C^2W-deny and influence operations, respectively. By the C^2W methodology of data denial, we can limit threat force ability to know and forecast the weather conditions in the joint task force area of operations, thereby increasing our ability to win the information war and out-maneuver and out-fight the enemy. Additionally, the enemy can be put at a disadvantage at a critical time and place if we could covertly modify their picture of the weather, thereby influencing them to take detrimental COAs. Also, possibilities exist for intercepting enemy weather data bases and transmissions without their knowing.

Training

Soldiers and units will fight as well or as poorly as they have trained. According to **FM 100-5, Operations**, small-unit training, physical conditioning, and discipline remains the most effective way to offset the adverse effects of the weather. Training in poor weather conditions builds confidence and teaches soldiers and commanders how to adjust to weather extremes.

The OTW training strategy involves incorporating advanced environmental technology and exploitation of weather into training, combat simulations (virtual, constructive, and live), weapons development, and system testing and evaluation. Experimenting and training with OTW concepts and technology in future Advanced Warfighting Experiments (AWEs) will enable commanders and soldiers to develop, test and practice tactics, techniques and procedures that will truly allow them to exploit the weather to their benefit and maximize our battlefield advantage in lethality, survivability and tempo of operations.

Incorporation of real weather scenarios and weather-effects information in combat models and simulations will dramatically increase the level of realism in the AWE environment. Leaders at all levels will experience the difference that the consideration of weather effects has on planning and executing operations of all types. Exercising these weather capabilities is key to getting leaders accustomed to including weather in the planning of operations at all levels. It will build confidence in the weather-data gathering, processing and planning capabilities available to them.

Conclusion

OTW is a vision for Force XXI battlefield weather operations. It leverages the power of weather information and technology to enhance deployment and sustainment, and to increase lethality, survivability, and the tempo of operations in war and other military operations. OTW is critical to seeing and out-thinking the enemy, gaining information dominance and winning the information war, and to controlling the environment (to permit continuous around-the-clock operations). It is essential for dominating maneuver forces and knowing target-area meteorological conditions needed to execute precision strikes.

OTW is truly a horizontal technology-integration initiative with major applications at all echelons and across the full spectrum of BOSs and functional areas. It is an integral part of digitizing the battlefield. It provides a "capability solution" to Army modernization which maximizes the capabilities of existing systems. OTW capitalizes on more than 25 years of shared Army effort and investment in meteorological research and development. It presents a low-cost, low-risk, high-payoff opportunity with a large battlefield return on the investment. The Army can realize the complete OTW capability within 10 years, just in time for Force XXI.

OTW is a crucial building block in the shaping of Force XXI according to **Army Focus 1994**. Force XXI commanders must have the ability to see throughout the depth of a dirty battlefield, cutting through bad weather and the fog of war with unprecedented detail, certainty, and in near-real time. We must own the environ-

(Continued on page 48)

CTC NOTES

Editor's Note: With this issue of ***MIPB,*** *we inaugurate a new department: CTC Notes. Each issue will contain articles by authors from one or more of the CTC's; the National Training Center (NTC), the Joint Readiness Center (JRTC), the Battle Command Training Program, and the Combat Maneuver Training Center (CMTC). This issue contains observations from both JRTC and NTC.*

Before JRTC—Effective S2 SOPs

by Lieutenant Colonel Michael T. Flynn

Over the past year at the Joint Readiness Training Center, our intelligence observer/controller (O/C) teams have seen continued improvement by brigade and battalion S2 sections. After observing numerous S2s during the last year, our O/Cs identified that success lies in developing and applying sound standard operating procedures (SOPs), based on doctrine and tested tactics, techniques and procedures (TTP). Experience shows that effective S2 SOPs cover six areas:

- ☐ Intelligence preparation of the battlefield (IPB).
- ☐ Reconnaissance and surveillance (R&S) planning.
- ☐ Staff integration and synchronization.
- ☐ S2 section operations.
- ☐ Asset integration with emphasis on intelligence and electronic warfare (IEW) assets.
- ☐ Intelligence support to the targeting process.

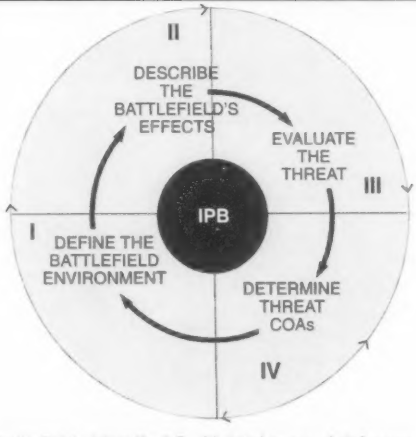
The following thoughts on these six areas are based on the doctrinal products that S2s can complete at the home station, as part of the "homework" phase of IPB (see Figure 1). Terrain analysis products, order of battle laydowns and OPFOR doctrinal templates should be completed well before deploying to Fort Polk, Louisiana.

Successful S2s prepare these in advance. They are thoroughly familiar with them before beginning the orders process at the Intermediate Staging Base (ISB), or at the home station for those units conducting an airborne insertion.

R&S remains a weak point throughout the force. Failures can usually be traced to two root causes: units do not follow their SOPs for R&S and commanders do not demand that R&S missions be planned as carefully as other combat missions. Those commanders who have planned and executed R&S missions with the same level of detail as they did any other combat operation have achieved great success at the JRTC. However, in a majority of cases, R&S operations are given short consideration in the planning process, and the results have been obvious and disappointing.

S2s at JRTC are not successfully participating in staff integration and synchronization of battlefield operating systems (BOSs). Successful S2s have aggressively tapped into the system of systems which a battalion or brigade task force (TF) brings to the fight. However, the majority of S2s overlook expertise available in their own tactical operating centers (TOCs). The best available source on threat BOS capabilities is usually the staff BOS representative.

S2 section operations should be driven by SOPs and staff battle drills. The goal when assessing your section operations is to measure the ability of your sec-



Step 1: Define Battlefield: Identify AO, AI, intel gaps, databases
Step 2: Describe Battlefield Effects: Weather, terrain, OCOKA; mobility corridors; NAIs, and TAIs
Step 3: Evaluate Threat: Doctrinal, situational templates, input to HVTs, HPTs
Step 4: Determine Enemy COAs: Event template and matrix, collection plan, specific info requirements, specific operational requirements,intel synchronization matrix, intel estimate

Figure 1. Intelligence Preparation of the Battlefield.

tion to conduct its essential tasks smoothly, without requiring so much key leader input and supervision that those leaders become distracted from the planning process.

Asset integration and utilization is a tough job, made all the more difficult by not understanding the capabilities of collection assets or how they are best employed. For the MI collection systems, S2s should talk to their supporting MI companies and battalions about the systems they bring to the field. To be successful, an S2 must also understand the capabilities of key collection assets which do not come from the MI side of the house. First, any maneuver S2 who does not understand how scouts function, and how difficult it is to get "eyes on" a target while avoiding detection, owes it to their Task Force to spend time in the field with the Scout Platoon. S2s must also learn the ranges, capabilities and employment of all potential collection assets within the TF.

Intelligence support to targeting provides the focus the staff needs to bring all fires, lethal and non-lethal, to bear against the commander's high pay off targets (HPTs). Some key considerations the S2 must keep in mind as he prepares for and participates in targeting meetings are as follows:

- ☐ Identify high value targets (HVTs) before the meeting and brief them as part of the S2 Intelligence update.
- ☐ Know what collection assets are available, and their limitations and capabilities.
- ☐ Be prepared to recommend HPTs.
- ☐ Be prepared to brief your Event Template and recommend which collection assets should be used to detects HPTs.

Successful brigade and battalion S2s at JRTC have all understood the central role that intelligence plays in their unit's success. Their ability to visualize the enemy and project enemy courses of action have been clearly presented. The bottom line is, strong S2s are willing to make tough calls and are able to synchronize their efforts with the rest of the staff to support the commander's plan.

Lieutenant Colonel Flynn is the Senior Observer/Controller for Intelligence at JRTC. He has a master's degree in Military Arts and Science from the School of Advanced Military Studies and a master's degree in Business Administration from Golden Gate University. He also holds a bachelor's degree in Management Science from the University of Rhode Island. Readers can contact him via E-mail flynnmt@polk-emh2.army.mil and call (318) 531-0199 and DSN 863-0199.

Advice for Maneuver S2s from NTC

by Captain David H. Stapleton and Major Thomas M. Smith

The primary goal of combat intelligence is to piece together battlefield information to determine enemy intentions. The direct support (DS) artillery S2 and the target acquisition targeting technician (131A) operating at the brigade fire support element can provide critical information in this endeavor. At the National Training Center, they are not currently tasked commensurate with their capabilities.

Maneuver Brigade S2s at the National Training Center (NTC) frequently fail to take advantage of the field artillery battalion as an intelligence collection agency. Soldiers of the artillery battalion can provide key pieces of combat information based on their unique artillery expertise and their access to information available from the AN/TPQ-36 and AN/TPQ-37 Firefinder radars. The Q36 and Q37 provide real-time intelligence on enemy indirect fire systems locations out to 24 and 50 kilometers respectively. This article will present several key intelligence indicators that first become available at the DS artillery tactical operations center.

The OPFOR at NTC frequently employs air-mobile insertions during offensive operations. In many cases, the maneuver brigade lists priority intelligence requirements (PIR) as "Where and when will the dismounted infantry land?" Krasnovian doctrine is similar to U.S. doctrine in that artillery targets are planned to cover primary landing zones (LZs). Given that the maneuver brigade S2 has templated potential LZs, as well as windows of

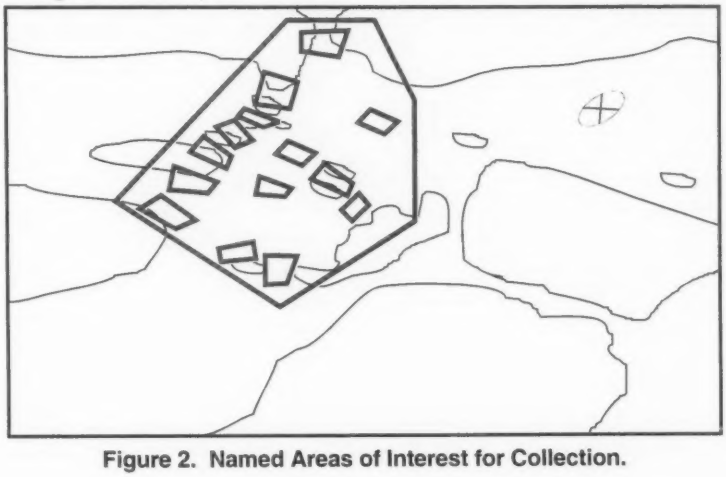


Figure 2. Named Areas of Interest for Collection.

opportunity for the insertion to occur, he can then assign these templated LZs (named areas of interest or NAIs) to the artillery battalion to observe for incoming enemy artillery fire. The artillery S2 can prepare his radar deployment order to ensure that the appropriate radar (Q36 or Q37) is cueing to detect preparatory fires on the landing zone.

Another common PIR at NTC is "When and where will the enemy fire persistent chemicals or the Family of Scatterable Mines (FASCAM)?" Again, the artillery battalion S2 with the attached Firefinder radar can answer this requirement. Special munitions such as FASCAM or persistent chemicals must be delivered with a large volume of indirect fire. Both the Q36 and Q37 will provide volumes of fire analysis, for example, a large number of acquisitions emanating from one location. The artillery battalion S2 can then determine, based on the friendly situation, why the enemy would employ a high volume of fire in a certain location. The Brigade S2 can facilitate this mission by tasking NAIs corresponding to templated special munitions targets, at the appropriate time, to the artillery S2.

The OPFOR Commander positions his artillery battalions within doctrinal distances of his forward line of own troops (FLOT). If we know the locations of either the enemy artillery battalions or the FLOT, we can couple this information with quick terrain analysis and deduce, with great accuracy, the location of the other variable. Again, the Firefinder radar can provide the location of enemy firing units. In almost every battle at the National Training Center, the artillery battalion S2 correctly identifies regimental and divisional artillery groups' locations. Unfortunately, in most cases, this information serves only to assist in planning for counterbattery targeting and is not passed to the brigade. Brigade S2s would benefit by tasking the artillery battalion for this information.

In Krasnovian operations, both defensive and offensive artillery fires are delivered in distinct, discernible phases. An understanding of which phase of fire the Krasnovians are firing may allow us to determine what action the enemy will take next. The DS artillery S2, based on analysis of all radar acquisitions, can determine the enemy phase of fire. Thus, he can determine **likely** enemy intentions. A clear example is Phase III Krasnovian fires in the offense: **fires in support of the attack**. These fires are focused primarily at the intended point of penetration. Phase III fires begin when the OPFOR begins the direct fire battle. The artillery S2, presumably aware that Phase III fires have been initiated, may be able to quickly discern the enemy's intended point of penetration.

Over-focusing Intelligence Collectors

S2s are constantly being told to "focus" their collection assets. In an attempt to do so, we have begun to **over-focus** assets by assigning more and more NAIs that are too small. The trend has been "under-employing" our collectors to their fullest extent (specifically their ability to think). For example, in Figure 1, the S2 has closely examined the terrain in the brigade sector and overfocused the collectors by employing a "measle sheet" NAI overlay. In the open and unvegetated terrain depicted, one observer can see nearly all (if not all) NAIs in the larger enclosed area. If the S2 **really** needs to know the enemy's route as he moves through the area between the large hill masses to the north and south, then that is what we need to tell our collectors to tell us—and assign an NAI encompassing the larger box. Some collectors may still require additional focus, and may indeed look at only one of the smaller NAIs, but at least consider a collector's ability to think and accomplish your **intended result** given its location on the battlefield. Our bottom line is to consider using larger NAIs when appropriate.

Captain Dave Stapleton is the DS Artillery Battalion S2 Trainer at NTC. He has a bachelor of science degree in Biology from Pennsylvania State and holds a master of science degree in Strategic Intelligence from the National Military Intelligence College. Readers can reach him at (619) 380-5524 or DSN 470-5524.

Major Smith is NTC Brigade S2 Trainer. He has a bachelor of science degree in Geology from the University of Oregon. You can reach him at (619) 380-4443/4673, DSN 470-4443/4673, and via E-mail at Bronco09@irwin.army.mil.

Owning the Weather

(Continued from page 45)

ment and the night, operating unrestricted in adverse weather .

General Gordon R. Sullivan, former U.S. Army Chief of Staff, said—

As we leap technologically into the 21st century, we will be able to see the enemy, day or night, in any weather—and go after him relentlessly. The technology is there, waiting for us to pull it all together. Own the night. Own the weather. Three minutes from sensor to shooter. Smart weapons, smart munitions. Decisive victory!

That statement really says it all.

Mr. Szymber is a meteorologist with the U.S. Army Research Laboratory (ARL) and serves as ARL's OTW liaison to the Intelligence Center. He has a bachelor's degree in Geography from Arizona State University and a master's degree in Atmospheric Sciences from the University of Arizona. Readers can contact him at (520) 538-0723/6472, DSN 879-0723/6472, and via E-mail at szymber@arl.mil.

CONCEPTS & DOCTRINE

The Intel XXI Concept III: The Seven Intelligence Tasks

by Captain Neal J. Wegner

*Editor's Note: In the April-June 1996 issue of **MIPB,** Captain Wegner began his three-part series on the Intel XXI concept. In this edition, he concludes the series, addressing the seven intelligence tasks neccessary to provide the warfighter with intelligence support.*

In the July-September 1996 issue of ***MIPB,*** I wrote about the Force XXI operational patterns and how these are the key to supporting the warfighter. Understanding these six operational patterns is essential for intelligence professionals. When we better understand how warfighters operate, we can more accurately focus our support to them.

This is the approach we took when writing the Intel XXI concept. From our understanding of the warfighters' operational patterns, we derived seven **intelligence tasks**. These represent what **must** be done to provide warfighters with dynamic and responsive intelligence support (see Figure 1). These seven tasks are—

- ☐ Direct.
- ☐ Collect.
- ☐ Analyze.
- ☐ Disseminate.
- ☐ Present.
- ☐ Attack (electronic).
- ☐ Protect.

We envision that these seven tasks will broaden, redefine, and possibly supercede those currently associated with the intelligence cycle.[1] They are neither linear nor cyclic, but instead must be continuously and dynamically performed in support of doctrinal intelligence functions.

Direct

In Force XXI, intelligence professionals will be required to **direct** the full range of intelligence and reconnaissance, surveillance, and target acquisition (RSTA) assets. These assets include not only organic collectors, but also joint, national, and multinational as well. Input from all battlefield sensors must be managed and fused to provide a dynamic, accurate picture of the battlespace. Consequently, intelligence operations must go beyond the traditional intelligence collection management activities and take into account the entire intelligence and RSTA domain. It is imperative that the senior intelligence officer be directly involved in planning, coordinating, synchronizing and directing the entire intelligence and RSTA effort. In other words, S2s and G2s must act as their commander's "chief of reconnaissance."

Intelligence analysis will support IO by focusing on the collection of intelligence on adversary C^4I capabilities and procedures

To effectively direct the intelligence and RSTA systems of the future, intelligence personnel must be able to dynamically plan, coordinate, and synchronize the intelligence and RSTA mission using visual displays, artificial intelligence, and automated synchronization matrices. They must also know the status and location of all available intelligence assets. Intelligence personnel must be able to see, in real-time, the execution of intelligence and RSTA operations. They must also be able to see and manage sensor-to-sensor and sensor-to-shooter linkages. Operators must know how to pass area and target coverage horizontally and vertically to other organizations. With such capabilities, intelligence elements will be able to dynamically task, retask, and shift the focus of intelligence and RSTA coverage and thus more effectively satisfy the reconnaissance and intelligence objectives of their commanders.

To dynamically "sync" and "resync" operations, commanders and staffs must also have a real-time view of the intelligence and RSTA operation while it is executed. Such current battle displays for the commander and staff must graphically present the intelligence and RSTA objectives as they are happening, and portray them in the context of the overall situation. With such capabilities, future commanders and their staffs will be able to more effectively direct and influence intelligence and RSTA operations and mass effects on the critical targets while maintaining the operational tempo (OPTEMPO).

Collect

Intel XXI **collection** systems will enable commanders to see their extended **battlespace** with great fidelity. These systems will provide commanders with the intelligence needed to understand their battlespace and to locate, identify and track critical targets. The sensor inventory will include multispectral-sensor-equipped combat vehicles, aircraft (both manned and unmanned), and soldiers.

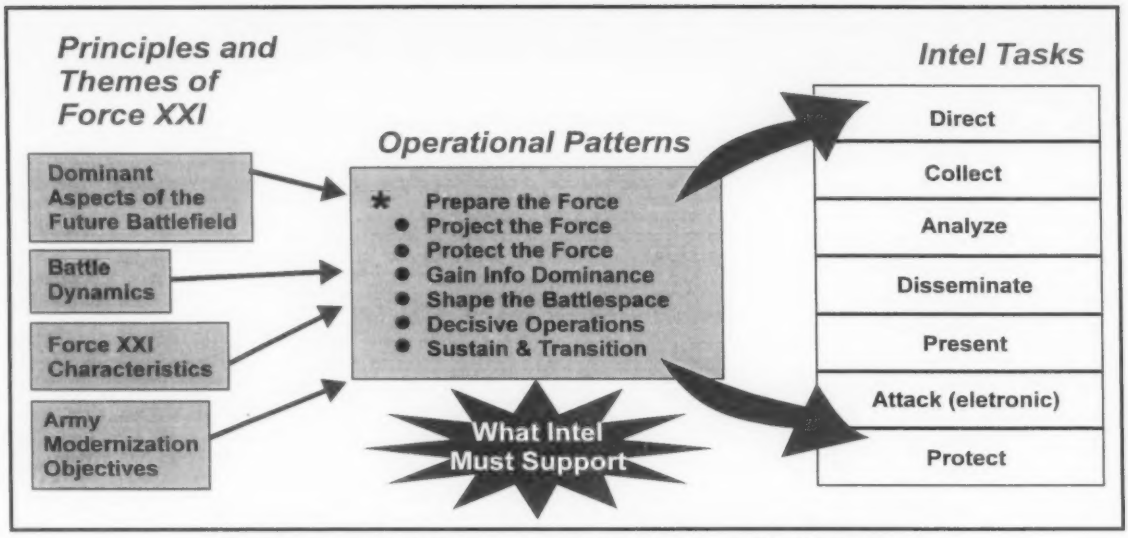


Figure 1. Intel XXI Tasks in Support of the Force XXI Warfighter.

The trend of future collection is for fewer, more modular and tailorable systems. They will be accurate, automated, and cover full spectra and wide areas. Unmanned aerial and ground sensors, to include robotics and microelectronic machines, will operate together to provide coverage in areas inaccessible to conventional collection means.

On the future battlefield, the individual solider will continue to be a critical component of the collection system. Information from front-line soldiers, special operations forces, long-range surveillance units, counterintelligence teams, interrogators, and other specialized human intelligence (HUMINT) operations, will be fused with data from high-technology sensors to answer the commander's priority intelligence requests (PIR). As demonstrated in Haiti and Bosnia, stability and support operations will require increased emphasis on HUMINT assets and soldiers operating on the ground to provide the required intelligence.

Analyze

Analysts convert battlespace information into intelligence and understanding to support effective decisionmaking. As the extended battlespace grows and the OPTEMPO increases, Intel XXI will provide systems common to all echelons for rapid processing, analysis, and output of intelligence and RSTA information. Analysis—including the processing of intelligence data while on the move—will be necessary to support our continuous operations. Future analysis capabilities will support the rapid and dynamic creation of the commander's picture. In the end, analysts must be able to make the enemy situation "come alive" so that commanders can quickly understand and act on what they see. The ability to rapidly analyze and process data will demand a system that provides a virtual connection between collectors and warfighters, with efficient filtering to prevent any information overload.

Intelligence analysis will support information operations (IO) by focusing on the collection of intelligence on adversary command, control, communication, computers, and intelligence (C^4I) capabilities and procedures. Understanding the adversary's decisionmaking process also can support accurate assessments of potential command and control (C^2) targets and targeting of critical nodes in synchronized attacks.

The operational value-added of such analytic capabilities will be more timely, relevant, and accurate battlefield visualization. It will provide the commander with the ability to understand threat force capabilities, vulnerabilities, and intentions in relation to the terrain, weather, and operational situation. It will rapidly turn information into understanding so that commanders can more effectively conduct decisive operations. Analysis is key to effective contingency planning, wargaming, rehearsal, and execution. It therefore supports all phases of operations during peacetime and conflict.

Disseminate

OPTEMPO and force dispersal require that commanders have an uninterrupted flow of, or access to, intelligence on the move. As operational forces disperse and conduct distributed operations, a robust and flexible **dissemination** means becomes a critical requirement. Without it, Intel XXI will not be able to provide commanders with timely visualization of their respective battlespaces.

Variations of "smart push-smart pull" technologies will provide the required information and allow automatic updates based on established search criteria. Automatic processing of requests for information (RFIs) will speed-up the process of answering the commander's PIR. If information is not immediately

available, the requester could access the status of ongoing actions in response to the request. Future technologies will allow dispersed processors to access available data without overburdening communications.

Dissemination is a key element of the intelligence process. No matter how much information is collected, processed, analyzed, and stored, intelligence is of no value unless it is available to combat commanders when they need it. The right intelligence and targets provided to battle commanders when they need them is the value-added of effective dissemination. This helps sustain the OPTEMPO, enhances lethality, and improves survivability.

Present

The future intelligence system under design will **present** an accurate and relevant high-fidelity intelligence picture of the battlespace, integrated with overall situation information including high-resolution weather and terrain data. This picture will convey an immediate understanding of the operational impact of the current and projected situation, including the impact of IO on the adversary's decisionmaking process. The production of this presentation is made by an organization of highly skilled, well-trained intelligence soldiers who analyze the threat, weather, and terrain within the context of the operational situation and the commander's intent.

Advanced presentation capabilities enable sustained OPTEMPO, enhanced lethality, and improved survivability.

The commander and staff's understanding of the battlespace and the enemy situation is fundamentally derived from a coherent and timely "picture" of the battlespace presented by the S2 and G2. This intelligence task encompasses battlefield visualization—the understanding of what the available information means in terms of the six dimensions of the battlespace:

- ☐ Width.
- ☐ Depth.
- ☐ Height.
- ☐ Time.
- ☐ Electromagnetic.
- ☐ Human.

Additionally, the commander's ability to anticipate difficult decisions, analyze options, and reduce uncertainty directly relates to his intelligence staff's assessment of future enemy actions and intentions in time and space. The portrayal of those actions during the wargaming process and the rapid unfolding of combat operations, will include live and virtual images which produce a dynamic and coherent picture of the battlefield. In addition to displaying the current location, size, and type of unit, the display will graphically depict the currently projected capabilities of an entity in terms of time and distance. Ultimately, the commander must understand the impact of what is presented and use that understanding to make **knowledge-based decisions**.

Future Intel XXI presentation capabilities represent a quantum leap in the intelligence system's support to the commander's ability to decide, act, resynchronize operations and focus his resources. Advanced presentation capabilities enable sustained OPTEMPO, enhanced lethality, and improved survivability.

Attack

The **attack** intelligence task supports the application of lethal and nonlethal means to high-payoff targets. It also includes attacking the adversary's decisionmaking process to prevent effective C^2 as well as the traditional intelligence targeting effort. Commanders require a thorough understanding of the adversary's C^2 structure and his decisionmaking process to effectively attack it. Detailed analysis, to include a thorough understanding of the military information environment developed in peacetime and updated during the all phases of the military operation, provides the foundation for understanding the adversary's information systems operations. This analysis forms the basis for developing and executing effective C^2 attack actions to destroy, disrupt, deny, or degrade adversary information networks, C^2 systems, information and intelligence sources, and decisionmaking processes.

Sophisticated nonlethal attack options to deny, disrupt, interrupt, interfere, distort or destroy information will be planned and executed in part by intelligence units as a key portion of the commander's C^2 attack strategy. Electronic attack (EA) options may range from surgically jamming the frequency spectrum to intrusion into C^2 systems to manipulate data. Command and control warfare (C^2W) battlefield damage assessment (BDA) is essential in assessing the effects of C^2 attack and maintaining information dominance. However, devising a means to conduct BDA on targets which have been nonlethally engaged poses significant challenges to future intelligence staffs.

EA is part of an integrated operation that helps the commander shape the battlespace, thereby enhancing our ability to achieve information dominance at the decisive moment. Its aim is to prevent the enemy from being able to react in time to our actions. Effective electronic attack operations will allow friendly forces to manage adversary perceptions, execute deception operations, and protect friendly forces and information.

Protect

Protect actions can be offensive or defensive in nature. Offensive protect uses all attack means (for example C^2W, physical) to reduce the adversary's ability to attack friendly C^2. It will place added emphasis on attack of multidisciplined RSTA systems and intelligence capabilities as the "eyes," "ears," and "brain" of the adversary attack capability. Defensive **protect** reduces friendly vulnerabilities to adversary attack by employing physical and electronic protection. Protective measures must be incorporated into Army systems as they are planned, designed, and developed. Failure to do so increases the risk to our forces. Our ability to thoroughly understand and graphically depict the IO battlespace is the basis for effective **protect** planning and execution. Protective actions allow commanders to effectively command and control their forces while optimizing their survivability and OPTEMPO.

Conclusion

In this series of articles, we began with an overview of Force XXI principles and the commanders' requirements. Recent operations in Haiti and Bosnia, among others, have given us a preview of the challenges that lie ahead and the wide range of missions our 21st century Army could face. We discussed how we must design, equip, and train the Intel XXI force to meet the commanders' needs in a resource-constrained environment with nontraditional missions and proliferating technologies and weapons. Our 21st century intelligence force must be flexible, tailorable, rapidly deployable, and capable of joint and coalition operations.

As we said earlier, the second part of this series covered six of the Force XXI warfighters' operational patterns. (There is a seventh pattern, **prepare**, which we did not discuss in that article.) We considered these patterns in our development of the Intel XXI concept .

The 21st century intelligence force will provide commanders with a knowledge-based, prediction-oriented capability that can meet their information and intelligence requirements. Central to this concept are quality soldiers, leaders, and civilians. Intel XXI represents a force that will—

- ☐ Produce timely presentations of their battlespaces for commanders, enabling an accurate understanding of the operational environment, adversary, terrain, and weather.
- ☐ Provide intelligence personnel with the resources necessary to conduct, coordinate, and synchronize intelligence operations in concert with supported operations.
- ☐ Equip the force with tailorable, multispectral collection capabilities to deal with emerging threats and technologies.
- ☐ Synchronize and leverage national intelligence and collection resources in support of operational decisionmaking.
- ☐ Support operations on the move using broadcast and smart "push-pull" technologies.
- ☐ Provide Force XXI with an effective weather capability by giving soldiers the information they need to fight and operate in all weather conditions.
- ☐ Support lethal and nonlethal attack targeting and execution through the synchronization of intelligence in IO and C^2W, seizing the advantages of information dominance.

Figure 1 displays the Intel XXI concept. The tasks are shown in conjunction with the operational patterns and the Force XXI principles and themes.

Endnote

1. The current doctrinal intelligence cycle is plan and direct, collect, process, produce, and disseminate. A discussion of this five-step process in intelligence operations is in **FM 34-1, Intelligence and Electronic Warfare Operations**, dated 27 September 1994, 2-15 throught 2-17.

Captain Neal J. Wegner is currently an action officer in Concepts Dvision, Directorate of Combat Developments at the U.S. Army Intelligence Center and Fort Huachuca. Readers can contact him via E-mail at wegnern@huachuca-emh1.army.mil and telephone (520) 538-2258/7213 or DSN 879-2258/7213 .

Evolution of FM 34-40 to IEW Support to C^2W

by Major Robert A. Peterson

Intelligence and electronic warfare (IEW) provides commanders with the ability to visualize the expanded battlespace in C^2W and to identify where and when they gain information dominance over an adversary. Through the Intelligence battlefield operating system (BOS) and other BOSs, information is collected and protected while the C^2W elements—operations security (OPSEC), psychological operations (PSYOP), deception, physical destruction, and electronic warfare (EW)—influence, disrupt, or stop adversary information flow.

Support for Information Dominance

The requirement for information and intelligence products on adversary capabilities and vulnerabilities to support information dominance is a basic intelligence function. Most of the intelligence tasks required to support C^2W are already known and practiced, but C^2W requires greater detail on adversary C^4I; decision makers, and their decision cycles. IEW capabilities must keep pace with evolving communications and information technology to ensure our continuing support to the commander.

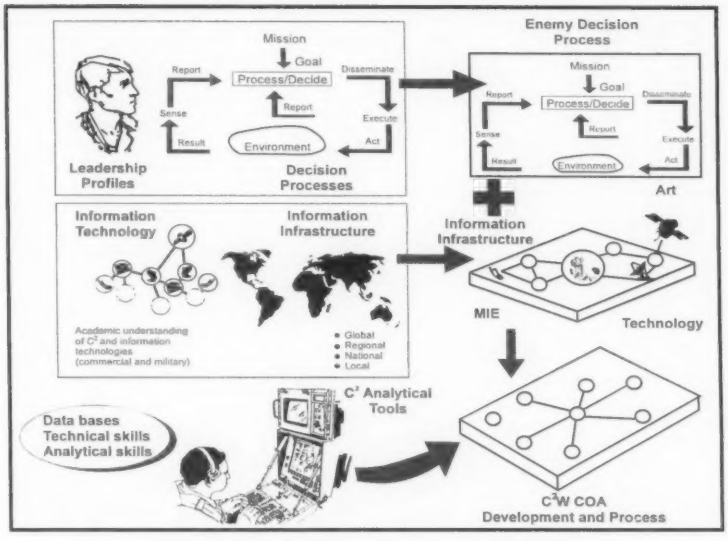


Figure 2. Understanding the Adversary.

The U.S. Army has historically trained and executed OPSEC, PSYOP, deception, EW, and physical destruction missions. To some extent, units synchronized some or all of these missions, and in turn, they were synchronized with intelligence. C²W requires the synchronization of all its elements and intelligence with maneuver to make information a successful combat multiplier.

Due to the elusive nature of the target—information, information communications systems, and sensors—intelligence analysts, whether they are all source or single source, require accurate and detailed data with which to develop their information and intelligence products. In order to support C²W, intelligence analysts must be diligent in peacetime to develop and maintain the requisite databases, estimates, and information or intelligence product sources to support the wide range of contingencies. As witnessed in Operations DESERT SHIELD and DESERT STORM, the deployment phase is not the time to find that you do not have the information available to support the commander.

For information and communications infrastructures, the difficulty in collecting, analyzing, and disseminating the intelligence to support IO and its subset, C²W, requires careful asset and requirement management to ensure satisfaction of the C²W intelligence requirements. The intelligence effort against information and communications infrastructures also needs to raise in priority to satisfy detailed C²W planning and execution requirements.

The New FM 34-40

The publication in August 1997 of a new **FM 34-40, Intelligence and Electronic Warfare (IEW) Support to Command and Control Warfare (C²W)**, continues the momentum of the U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH) in evaluating the impact of IO at the operational and tactical levels. The evolution of **FM 34-40, Electronic Warfare Operations** (November 1987), to **IEW Support to C²W**, indicates the requirement to synchronize the five elements of C²W. Units have to synchronize OPSEC, PSYOP, military deception, physical destruction, and EW in an environment where information systems and communications technology continues to make rapid advances. The manual ties together IEW with C²W in the following areas:

- ☐ Information operations and C²W terminology.
- ☐ G2 and EW officer roles in the C²W staff.
- ☐ IEW in the C²W planning process.
- ☐ Intelligence support to C²W.
- ☐ Tactical HUMINT, imagery intelligence, measurement and signatures intelligence, and signals intelligence and electronic warfare considerations in C²W.
- ☐ The supporting agencies for Army IO and C²W.

The new publication follows on the heels of **FM 100-6, Information Operations** (August 1996), and **Joint Publication 3-13.1, Joint Doctrine for Command and Control Warfare** (February 1996). The soon-to-be-published **FM 101-5, Staff Organization and Operations** also provides insight into C²W by introducing a new operations order C²W annex that incorporates OPSEC, PSYOP, military deception, and EW. Physical destruction, the fifth C²W element, remains in the fire support annex with offensive EW (for example; jamming). It is critical that the C²W annex and the fire support annex with its C²W physical destruction element be cross-checked and the tasks deconflicted.

Major Peterson is the Executive Officer, 305th MI Battalion at Fort Huachuca, Arizona. He served as an instructor for the MI Officer Basic and Advanced Courses and the 35G assignment-specific training course. Major Peterson has also served with the 741st MI Battalion, 751st MI Battalion at Field Station, Korea; and the 504th MI Brigade. He holds an administrative science master's degree in Information Technology Management from Johns Hopkins University and a bachelor's degree in Computer Science from Texas A&M University. Readers can contact him via E-mail 102415.2325@ compuserve.com, (520) 533-6839, and DSN 821-6839.

Recommended Reading List for Company Grade Officers

Foundation Reading List

Company grade officers are required to read ten books as indicated below:

☐ **General History** (read 1):

— Weigley, Russell F., **The American Way of War: A History of U. S. Military Strategy and Policy** (Bloomington: Indiana University Press, 1977).

— Heller, Charles E. and Stofft, William A., Eds. **America's First Battles 1776-1965** (Lawrence: University Press of Kansas, 1986).

☐ **Sustainment** (read 1):

— Creveld, Martin Van, **Supplying War: Logistics from Wallenstein to Patton** (New York: Cambridge University Press, 1979).

— Huston, James A., **The Sinews of War: Army Logistics 1775-1953, Army Historical Series** (Washington, DC: Office of the Chief of Military History (CMH), U.S. Army, 1966), **CMH Pub 30-4**.

☐ **Technology** (read 1):

— Brodie, Bernard and Fawn M., **From Crossbow to H-Bomb** (Bloomington: Indiana University Press, 1973).

— Creveld, Martin Van, **Technology in War: From 2000 B.C. to the Present** (New York: Free Press, 1988).

☐ **Training** (read 1)

— Collins, Jr., Arthur S., **Common Sense Training: A Working Philosophy for Leaders** (Novato, CA: Presidio Press, 1979).

☐ **Command and Leadership** (read 2):

— Rommel, Erwin, **Attacks** (Vienna, VA: Athena Press, 1979).

— McDonough, James R., **Platoon Leader** (Novato, CA: Presidio Press, 1985).

— MacDonald, Charles B., **Company Commander** (New York: Bantam, 1984).

☐ **Nature of War, Tactics, and Warfighting** (read 3):

— Swinton, Ernest D., **The Defense of Duffers Drift** (Garden Park, NY: Avery Publishing Group, 1986).

— MacDonald, Charles B., **A Time for Trumpets: The Untold Story of the Battle of the Bulge** (New York: Bantam, 1985).

— Keegan, John, **The Face of Battle** (New York: Penguin, 1983).

— Ryan, Cornelius, **A Bridge Too Far** (New York: Pocket Books, 1984).

— Ryan, Cornelius, **The Longest Day** (New York: Pocket Books, 1984).

— Sajer, Guy, **The Forgotten Soldier** (Elmsford, NY: Pergamon Press, 1967).

☐ **Low Intensity Conflict** (read 1):

— Race, Jeffrey, **War Comes to Long An: Revolutionury Conflict in a Vietnamese Province** (Berkeley: University of California Press, 1972).

— Downs, Frederick, **The Killing Zone: My Life in the Vietnam War** (New York: Berkley Publishing Group, 1987).

— Fall, Bernard, **Street Without Joy** (New York: Schocken Books, 1972).

Suggested Reading List

☐ **Classical**

— Blumenson, Martin, **The Patton Papers, Volumes 1 and 2** (Houghton and Mifflin Company. 1972 and 1974).

— Catton, Bruce A., **A Stillness at Appomattox** (Garden City, New York: Doubleday and Company, 1953).

— Cosmas, Graham A., **The United States Army in the Spanish-American War** (University of Missouri Press, 1971).

— Dupuy, R. E. and Trever, **Brave Men and Great Captains** (Hero Books, 1984).

— Fehrenback, T.R., **This Kind of War: A Study in Unpreparedness** (New York: MacMillan, 1963).

— Grant, Ulysses S. **Personal Memoirs, 2 Volumes**, 1894, [Reprint, 2-volumes-in-1] (New York, NY: AMS Press, Incorporated, 1978).

— Lewis, Lloyd, **Sherman: Fighting Prophet** (New York: Harcourt, Brace and Company, 1932).

— Marshall, Samuel Lyman Atwood, **Ambush: The Battle of Dau Tieng** (Nashville, Tennessee Battery Press, 1983).

— Marshall, Samuel Lyman Atwood, **Men Against Fire: The Problem of Battle Command in Future War**, 1947 [Reprint] (Gloucester, Massachusetts: Peter Smith, 1978).

— Shaara, Michael, **Killer Angels** (New York: Ballantine Books, 1976).

— Solzhenitsyn, Alexander, **August 1914** (New York: Farrar, Strauss and Giroux, 1972).

☐ **Ethical**

— Barnett, Corelli, **The Swordbearers: Supreme Command in the First World War** (Indiana University Press, 1975).

— Forester, C. S., The General, 1936 [Reprint] (Nautical and Aviation Books, 1982).

— Goulden, Joseph C., **Korea: The Untold Story of War** (New York Times Book, 1982).

— Halberstam, David, **One Very Hot Day** (New York: Warner Books, 1984).

— Hemingway, Ernest, **For Whom the Bell Tolls** (New York: Scribner, 1940).

— Karsten, Peter, **Law, Soldiers, and Combat** (Westport, Connecticut: Greenwood Press, 1978).

— Larteguy, Jean, **The Centurions** (E. P. Dutton and Company, 1962).

— Marshall, S. L., **The Armed Forces Officer** (U.S. Army, **DA Pamphlet 600-2**, same title).

— Peers, William R., **The My Lai Inquiry** (New York: Norton, 1979).

☐ **Contemporary**

— Ambrose, Stephen E., **Eisenhower: The President** (New York: Simon and Schuster. 1984).

— Blair, Clay, **Korea, The Forgotten War** (Times Books, 1987).

— Hapgood, David and Richardson, David, **Monte Cassino** (St. Martin's Press, 1984).

— Harvard Nuclear Study Group, **Living With Nuclear Weapons** (Harvard Press, 1983).

— James, D. Clayton, **The Years of MacArthur: Triumph and Disaster 1945-1964, Volume 3** (Houghton and Mifflin Company, 1985).

— Terry, Wallace, **Bloods: An Oral History of the Vietnam War By Black Veterans** (Random House, 1984).

— Wood, W. J., **Leaders and Battles: The Art of Military Leadership** (Presidio Press, 1984).

PROPONENT NOTES

Officer Issues—Implementation of CPT-PME

On 31 July 1996, Headquarters, Training and Doctrine Command directed the revision of MI OAC class schedules to support the implementation of Captain–Professional Military Education (CPT-PME). CPT-PME provides a professional development step for all officers earlier in their careers.

This change begins the transition from the current TDY-and-return home Combined Arms and Services Staff School (CAS^3) schooling for officers. Effective early in calendar year 1997, OAC graduates will attend CAS^3 at Fort Leavenworth, Kansas, immediately following OAC graduation in a TDY-and-return-to-Fort Huachuca status. The MI Branch Captains' Assignment Officer will continue to schedule officers for additional skill training (AST) courses (for areas of concentration: 35C Imagery Intelligence Officer, 35E Counterintelligence Officer, and 35G Signals Intelligence/Electronic Warfare Officer), either before or after CAS^3 (based on the officer's projected assignment and course seat availability).

CPT-PME alleviates the situations in which officers cannot attend CAS^3 during a tour, usually due to mission requirements and officer shortages in units. Those MIOAC graduates who have not yet attended CAS^3 must still do so at the earliest possible time. The OCMI POC is Captain D. A. Dannewitz; readers can reach him at (520) 533-1180, DSN 821-1180, E-mail dannewitzd@huachuca-emh1.army.mil.

Warrant Officer Accession Update

The OCMI has forwarded the warrant officer accession goals for the upcoming year to U.S. Total Army Personnel Command. Key elements of the accession plan are—

- ☐ A significant increase in the number of accessions in MOS 350D Imagery Intelligence Technician.
- ☐ The closure of MOS 352D Emitter/Location Identification Technician and 352H Morse Intercept Technician accessions for one year.
- ☐ Accessing applicants for MOS 351E Interrogation Technician and 352G Voice Intercept Technician by specific language. Current priority is for applicants with proficiency in Arabic, Korean, Persian-Farsi, and Chinese Mandarin. Personnel with other languages may still apply, but they may have to agree to retrain into one of the languages listed if selected for warrant officer accession.
- ☐ Continued high accession opportunities to fill projected shortages in MOS 350B, the All-Source Intelligence Technician, and 351B, Counterintelligence Technician.

The basic requirements to apply are listed in **AR 135-100, Appointment of Commissioned and Warrant Officers of the Army.** Specific requirements for each MOS are listed in **DA Circular 601-94-1, Warrant Officer Procurement Program.** This will be updated and sent to the field in the second quarter, fiscal year 1997. Accession boards for MI applicants are normally scheduled for the third weeks of January, March, July, and September.

Applicants should forward their packets to the U.S. Army Recruiting Command at least 45 days prior to the convening date of the board. Those interested in applying should discuss the procedure with a warrant officer in the applicant's career field or contact the OCMI POC Chief Warrant Officer Five Rex A. Williams, MI Warrant Officer Professional Development Manager, (520) 533-1183, DSN 821-1183, and E-mail address williamr@pentagon-hqdadss.army. mil.

MI CORPS HALL OF FAME

by Second Lieutenant Stephen P. Merchant, Jr.

Lieutenant Colonel Mercedes O. Cubría, (Deceased)

Lieutenant Colonel Mercedes O. Cubría (1903-1980) was inducted into the Military Intelligence Corps Hall of Fame in 1988 following a long and productive career with various assignments in Panama, Germany, France, Japan and England. During her 20-year career, she supported both MI and humanitarian assistance.

Lieutenant Colonel Cubria was born in Guantánamo, Cuba, to parents of Spanish and Cuban descent. At the age of 13 she came to the United States, and in 1943, enlisted in the Women's Auxiliary Corps (WAC) to help the war effort.

In 1943 she was commissioned as a second lieutenant and sent to Oxford, England, for

Photo provided by Frank de Varona

codes and ciphers training. Following her graduation, she became the security officer for the 385th Signal Company and then the 322d Signal Company for the remainder of World War II. Lieutenant Colonel Cubria was the first Army WAC officer to serve in the Caribbean Area—as a captain, she was assigned to the Headquarters of United States Army Caribbean, Quarry Heights, Panama Canal Zone.

After being awarded the Bronze Star for meritorious achievement in ground operations against the enemy, she became ill in 1953 and left military service.

In 1962, the Army needed personnel with cultural expertise of the Caribbean area. Major Cubría was a logical choice and was recalled to active duty. Her principal job was to interview thousands of Cuban refugees and to prepare detailed reports for MI and the Central Intelligence Agency. Major Cubría spent what spare time she had in assisting hundreds of refugees in finding work, housing, and education.

For her actions during the crisis in Cuba, Major Cubría was awarded the Legion of Merit and promoted to Lieutenant Colonel in 1968. Upon her second retirement in 1973, she was awarded the Legion of Merit with First Oak Leaf Cluster.

Lieutenant Colonel Cubría has served as a role model to millions of immigrants who have come to the United States in search of a better life. She is part of a great tradition of Hispanic Americans who have contributed to the defense of the United States and to humanity in general.

Second Lieutenant Merchant is currently working in the OCMI prior to attending the MI Officer Basic Course. Readers can contact him at (520) 533-1180, or DSN 821-1180.

RESERVE COMPONENT

New USAR MI Unit Structure

This is the fourth in a series of articles on the military intelligence (MI) Proponent-sponsored MI Reserve Component (RC) Force Design Update (FDU). The focus of this piece will be the U.S. Army Reserve (USAR) MI unit force that is currently in carrier status, scheduled to formally activate in fiscal year 98. The new USAR structure is built to answer the Active Component's (AC) requirement for wartime intelligence augmentation at the corps and theater level. Elements formerly aligned with the Army National Guard's combat divisions and brigades have been deactivated in the USAR. In the future, the Guard will "own" the MI structure that supports its tactical combat forces.

The new USAR units will be of a cellular or modular construct, designed to mobilize down to the team level via derivative unit

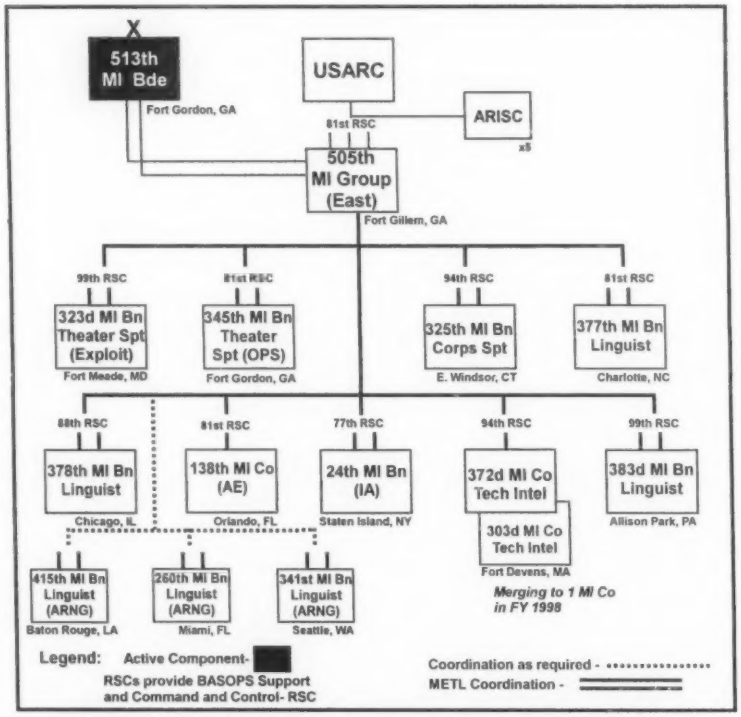


Figure 1. The USAR Major Regional Contingency-East.

identification code (UIC). The USAR MI force will afford the AC the capability to go to a higher operating tempo with a more robust capability; literally providing the second and third shifts critical to sustained operations.

The whole structure will move to a nearly pure MI military occupational specialty structure. Personnel will be assigned to MI functional teams. Training will focus to the team level. Equipment will be downplayed. If required for peacetime training, the reservists will, in main part, be assigned with existing AC intelligence and electronic warfare equipment. This was one primary factor in the stationing plan. In short, the USAR's contribution will be agile, available on short notice, adaptable and flexible. Mobilizing to the team level puts the RC contribution into theater early in the fight.

The redesigned USAR force falls into two major regional contingency (MRC)-focused groups aligned against the requirements of the U.S. Army Intelligence and Security Command (INSCOM) Force Projection Brigades (FPBs), the AC Corps and the theater. Each MI FPB has a supporting RC MI Group.

The 505th MI Group (East), Fort Gillem, Georgia, mobilizes to the 513th MI Brigade (FPB-E). The 513th supports four geographic commanders in chief (CINCs); U.S. Central Command, U.S. Atlantic Command, U.S. European Command, and U.S. Southern Command. MRC-East theater and corps requirements are answered by a single USAR corps support battalion (East Windsor, Connecticut) and two theater support battalions (Fort Meade, MD and Fort Gordon, Georgia). The language requirements for MRC-E are answered, in part, by three USAR linguist battalions located in Chicago Illinois, Charlotte, North Carolina, and Allison Park, Pennsylvania. The 505th is also has two technical intelligence (TECHINT) companies stationed

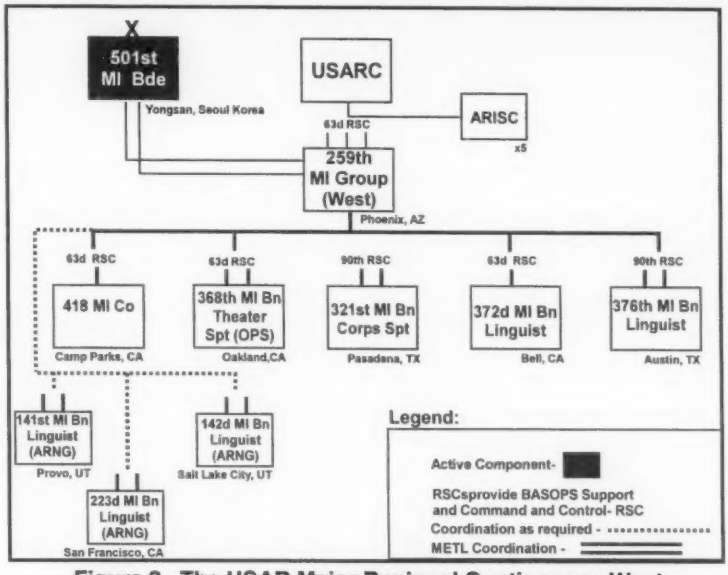


Figure 2. The USAR Major Regional Contingency-West.

at Fort Devens, Massachusetts, an imagery analysis battalion on Staten Island, New York, and an aerial exploitation company in Orlando, Florida. See Figure 1.

The 259th MI Group (West) in Phoenix, Arizona, has a mobilization responsibility to the 501st MI Brigade (FPB-W). Particulars regarding the 501st's responsibilities in the Pacific region are still evolving. MRC-W theater and corps requirements are captured in a single theater support battalion (Oakland, California) and a single corps support battalion (Pasadena, Texas). The MRC-W language shortfalls are provided, in part, by two USAR linguist battalions in Bell, California, and Austin, Texas. The 259th also has a small imagery analysis company. See Figure 2.

The peacetime command and control (C^2) of these units currently runs through the Regional Support Command (RSC) in which the unit resides. The next level of C^2 is the U.S. Army Reserve Command (USARC).

The close RC to AC relationship inherent in this structure derives from the original concept in which each individual element of the new structure exists because of a specific AC requirement for wartime RC augmentation. The AC's corps and theater requirement literally defines the size and composition of the new USAR MI force. This requirement trace will answer most of the RC corps and theater support battalion's questions regarding Mission Essential Task Lists, annual training sites, contributory support missions, training focus, and mobilization coordination contacts. The success of this structural initiative hangs, in large part, on the ability of the AC and RC to marry a specific AC requirement to an identified RC MI augmentation element.

Knowlton Award

The first presentation of the coveted Knowlton award to a commissioned USAR officer was made to Colonel Michael Capitman. Colonel Capitman most recently served in the senior Army Guard and Reserve MI position as Reserve Components' Advisor to the Army's Deputy Chief of Staff for Intelligence. His career spans almost 30 years of active, reserve and AGR MI service beginning in Vietnam with the 1st Infantry Division. He has commanded at the USAR unit level and served in varied

staff positions at U.S. Forces Command, INSCOM, and the Pentagon. Colonel Capitman is largely responsible for the USAR's assumption of the contributory support mission which will have reservists working real intelligence missions in support of the CINCs.

Colonel John Craig is the USAR POC and Chief of the Reserve Forces Office. Readers can contact him at (520) 533-1176, DSN 821-1176, and via E-mail at craigj@huachuca-emh1.army. mil.

Major Steve Ponder is the ARNG POC; his telephone number is DSN 821-1177 and his E-mail addresses are ponders@aol.com and ponders@huachuca-emh1.army.mil. Their fax number is 821-1762 and the mailing address is Commander, USAIC&FH, ATTN: ATZS-RA, Fort Huachuca, AZ 85613-6000.

PROFESSIONAL READER

Strategy and Tactics of the Salvadoran FMLN Guerrilla: Last Battle of the Cold War, Blueprint for Future Conflicts by José Angel, Moroni Bracamonte, and David E. Spencer (Westport, Connecticut: Praeger Publishers, 1995), 216 pages, $59.95.

This book is an outstanding reference tool for the MI professional who wants to understand guerrilla warfare as it is practiced today. This book is applicable beyond Latin America because the situation in El Salvador was watched closely by guerrilla organizations around the world who learned new tactics, techniques, and procedures (TTP) from the FMLN. Tactics from the FMLN continue to surface around the world including in Mexico, Guatemala, and Somalia. In fact, the Somali military chief responsible for the downing and damaging of three U.S. helicopters on 3 October 1993 claims to have learned the techniques from the FMLN. The reader should know that soldiers from Task Force Ranger dispute this claim.

The authors describe the FMLN's strategy for a prolonged popular war and various attempts at its implementation. They also describe in detail the make-up of the FMLN's five war fronts and their support structures. Offensive tactics are illustrated, with several examples of operations conducted throughout the war, including both ambushes and night operations. They devote an entire chapter to urban tactics complete with drawings of FMLN urban defensive operations. The chapter on defensive tactics discusses air defense operations, and includes anti-airlanding operations and an FMLN-developed antiaircraft sight for small arms weapons. It further describes FMLN-produced mines and their employment and descriptions of FMLN security procedures for setting up guerrilla camps.

An item of particular interest to the MI officer is the description of a communications system employed by the FMLN called the "strategic bridge." Using this system, messages from a headquarters are sent in plain text via land line to an observation post (OP), located up to three kilometers away. The OP then encodes the message and transmits it via radio. Salvadoran units often located the site of the radio transmission and attacked it with air-mobile forces, only to find just an OP. Meanwhile, the headquarters, with ample warning, displaced to a safe location.

This book is valuable for understanding the tactics of guerrilla forces worldwide, particularly in Latin America. Its topic and timeliness make it a good update for previous readers of Ché Guevara's **On Guerrilla Warfare**.

Captain Christopher J. Courtney
Fort Huachuca, Arizona

Cyberwar: Security, Strategy and Conflict in the Information Age by Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden (Fairfax, Virginia: AFCEA International Press, 1996), 298 pages, $24.95.

Whoever controls access to information will have the power in tomorrow's society. The world is currently on the brink of the"Information Age," a time when information technology will further advance beyond imagining. **Cyberwar: Security, Strategy and Conflict in the Information Age** is an anthology that describes the evolution of information and the capabilities and limitations of information in tomorrow's world.

Cyberwar shows how the history of information, from ancient times through the 20th century, has led to the information age of today. As class systems such as nomads, farmers, and hunter-gatherers evolved, communication facilitated group structure. Communication aided organization and helped societies transfer ideas, stories, and information to succeeding generations through the writings of scribes. In the Middle Ages, the Roman Catholic Church started the first era of information. The Church provided the catalyst for the spread of information, not only because it promoted individual development, but also because it funded, through tithes, the development of technology. Also, its scribes used written transcripts to consolidate ideas and technological advancements, thus spreading information. Eventually, the printing press provided society with the means to record information in many documents, which furthered the spread of information. In the 20th century, the recent development of the Internet has surpassed the technology of the telephone and telegraph. This digital revolution has further widened the spectrum of information capabilities, nearly beyond bounds.

Cyberwar suggests that businesses must become aware of the vast capabilities that the digital revolution has to offer. The speed of information transfer provides businesses a near-real-time capability to access information. The Internet is providing businesses with the ability to access a sea of information at the press of a few keys.

As in the business world, **Cyberwar** shows how new developments in information technology are providing U.S. military forces with a superb intelligence infrastructure. If U.S. forces are able to defeat potential threats in advance of physical engagement, not only do they neutralize the enemy without casualties, but they also limit costs. Not only does a strong information warfare (IW) capability prevent the high costs of troop deployment, it also lessens the need for a large inventory of backup weapons. Evolving information capabilities also provide U.S. forces a timely strategy for managing logistics and inventory requirements. Also, technology has provided U.S. forces with increasingly better intelligence. With such developments as the All-Source Analysis System, unmanned aerial vehicles (UAVs), and the Joint Surveillance Target Attack Radar System (Joint STARS), information and electronic warfare capabilities will increase. Intelligence analysts project that by 2005, U.S. forces will be able to identify 75 percent more of important threat targets on the battlefield than they did in Operation DESERT STORM.

Cyberwar suggests IW strategies, such as neutralizing an enemy from the center of his infrastructure. If threat commanders cannot receive information from higher headquarters, they cannot effectively manage their forward units.

With increased technological capacity comes increased technological dependence and a need for precautions. In the future, a nation without an IW capability will be a nation without a military capability. To ensure a potent IW strategy, however, the **Cyberwar** authors suggest that information users be aware of the limitations of cyberspace, the battlefield for future conflicts. These suggestions are just a few of those of which an information-based society should be aware. First, users should make multiple copies of information to prevent information warfare attacks, such as viruses and "infobombs" that target specific computers or bits of information. Second, users should use encryption and passwords to prevent hackers and potential threats from accessing classified or private information. Third, users should be aware of

the media's ability to distribute news globally in real-time, news that significantly impacts how adversary leaders perceive the United States. Thus, **Cyberwar** suggests the implications of "software," the ability of television to "shape a nation's will." Fourth, users should know about the impacts of propaganda through subliminal messages and digital manipulation. For example, the image of Forrest Gump shaking hands with several U.S. presidents suggests the ability to vastly distort information. Fifth, the United States must be aware that as information becomes more available, the possibilities for less advanced nations to harm the United States through IW increase. Sixth, users should continually troubleshoot their information systems to identify vulnerabilities. Finally, our legal system should impose increasingly severe legal liabilities for information attacks to further dissuade potential IW perpetuators. Clearly, an IW defense may be even more important than an IW offense.

Cyberwar, while illustrating the evolution of information, provides key insight on the capabilities and potential threats in the cyberspace world. This anthology provides informative accounts from several individuals with distinguished intelligence careers, such as U.S. Air Force Colonel (Retired) Alan D. Campen, Douglas H. Dearth, and Dr. R. Thomas Goodden. Furthermore, the authors contribute well-written, easy to understand chapters of which today's information users need to be aware, especially since information availability will only increase. **Cyberwar** estimates that in 2015, there will be 5,000 times more information in the world than there was in 1994. The authors clearly show the importance of preparing for and understanding such a world.

2LT James B. Osborne, Jr.
Fort Huachuca, Arizona

Great Battles and Leaders of the Second World War: An Illustrated History, Introduced by John Keegan (Boston and New York: Houghton Mifflin Company, 1995); 328 pages, $40.

Much has been written and will continue to be written about the horrors of World War II. John Keegan introduces **Great Battles and Leaders of the Second World War: An Illustrated History** to a new generation of readers. This collection of historical narrative presents an intensely personal accounting of events from behind the scenes, as recorded by Winston Churchill in his "epic six-volume history of the pivotal event of our century." More than 417 black-and-white photographs and 23 situation maps, many of which have never before been published, graphically recreate key episodes as Churchill recalled them.

Churchill contacted "key players," seeking their recollections and papers and soliciting their comments on his impressions. He also assembled a team of advisors to confirm dates, times, places, and personalities; he began his writings in 1946 and completed them in 1953.

Churchill concluded that **The World Crisis**, his five-volume history of World War I, and **The Second World War** journals, together formed—

an account of "another Thirty Years War" and an expression of his "life-effort" on which he was "content to be judged."

Unlike Roosevelt, Stalin, and Hitler—who did not leave any first-hand narrative of their involvement in World War II—Winston Churchill's "unique and acutely revealing" chronicle of events, meetings, debates, and disagreements with "a world of people" heralds the thin line he balanced with friends and foe alike. It is evident from this book that Winston Churchill was fascinated with military operations, following their progress closely, and that he employed TTP intended to defeat Hitler and Mussolini.

Winston Churchill poignantly wrote that he—

never criticized any measure of war or policy after the event unless [he] had before expressed publicly or formally [his] opinion or warning about it.

His life script as he lived it and exemplified in how he recorded it, portrays then and now a man of character, conviction, and foresight.

This account of Winston Churchill's is a comprehensive and intimately personal point of view from a legendary statesman. The book starts with the attack on Poland in 1939 and continues through all the battles, up to the campaign in Italy in 1944, and the dropping of the Atomic Bomb in 1945. In this book, too, are Churchill's frank opinions of himself and other prime ministers, heads of state, generals, ambassadors, and diplomats.

I highly recommend this book to all history buffs. The lessons learned in the accounting of World War II as it evolved and from actual notes and perspective of a primary leader are rare.

JoNell M. Elkins
Fort Huachuca, Arizona

The Lessons of Modern War, Volume IV: The Gulf War, by Anthony Cordesman and Abraham H. Wagner (Boulder, Colorado: Westview Press, 1996); $98.00 hardback $23.95 paperback.

This is possibly the most comprehensive critical analysis of Operations DESERT SHIELD and DESERT STORM in print. The continuation of Anthony Cordesman's series is worthwhile reading despite some basic research flaws that detract from the credibility of the book. Mr. Cordesman is a former Defense Department staff member and an expert in Middle-Eastern affairs.

Volumes One through Three address the Arab-Israeli Wars, the Iran-Iraq War, and the conflicts occurring in the Falkland Islands and Afghanistan. The books give a history of the conflict and a comprehensive "lessons learned" evaluation covering almost every battlefield operating system, major pieces of equipment, and other relevant issues.

In Volume Four, Cordesman covers lessons of the Gulf War. He addresses strategic, tactical, technical and human issues. This overview introduces specific sections, including a historical framework of the conflict; forces engaged; command, control, communications and computers; intelligence; the air and ground campaigns; naval warfare; missiles and proliferation; and strategic implications. This in-depth overview covers each conflict from formulation of strategy to the performance of specific weapons systems.

I **liked** this book. However, there are errors in Cordesman's research that detracted from the work's true value. Cordesman incorrectly writes that the corps MI brigades and divisional MI battalions were thrown together just in time to provide support for the war, and that they were inadequate at all levels. He is equally incorrect when he refers to then BG John Stewart as the Chief of Staff of the Army who took over the J2 position at Army Forces Central Command (ARCENT). These errors showed a lack in attention to detail that left me wondering where else similar mistakes were made.

I found these and a couple of other "slips" secondary as Cordesman conducts an extended and critical review of the problems in battle damage assessment, imagery dissemination and the performance of Joint STARS and the Pioneer UAV. He accurately points out the contributions made by these systems and conversely, their shortcomings indicating the need for improvements or new systems. This section is worthwhile reading for every intelligence professional as it highlights the good and the bad of key processes and systems.

Cordesman then takes the reader on a day-by-day account of the war that appears accurate. New light is shed on the contributions of SIGINT in determining the movement and actions of the Republican Guard units. This is something that I have not seen discussed in any previous work. His description of Iraqi plans, intentions, and the reasons behind their tactical decisions is simply the best of any book covering the Gulf War.

A critique that starts with land warfare systems and doctrine follows. This section is equally well written and will interest anyone wondering how well the M-1A1 Abrams tank, AH-64 Apache helicopter, and other systems performed. Naval and amphibious systems also get the same treatment. Air Force readers are most likely to be unhappy with the book as Cordesman really questions airpower effectiveness, supporting his statements with multiple sources including the Air Force's own study on the conflict.

The book is well footnoted and a comprehensive set of primary sources was used. While the reader will probably not agree with all of Cordesman's analysis, he **does** bring new points and criticisms to the field. It is refreshing to see a critical analysis and comprehensive history like this in print, compared to the less well-researched books that preceded it. Professionals from all branches and Services will benefit from reading this book.

CPT James C. Laughrey
Bolling Air Force Base, Washington D.C.

Application of Power

(Continued from page 16)

ian and military deaths in World Wars I and II, and the prospects of thermonuclear annihilation during the Cold War era.

It is equally difficult, however, to foresee the end of total war in a world increasingly dominated by technology. In the future, it might be possible for technologically sophisticated societies to truly wage war against the very fabric of the opponent's society—and to do so digitally. For generations now, we have witnessed indiscriminate attacks against civilian populations by military forces. The world likely will not be spared the genocide in Rwanda, the senseless waste in Liberia, or the religio-ideological destruction of Afghanistan. In the future, it may be increasingly difficult to detect the attacker—and indeed perhaps from what quarter and for what purpose. One could envision a politico-military future in which irregular warfare might be possible on an unprecedented scale. The targets (our's or their's) need not be physical infrastructure, but a nation's financial, automated distribution, and communications systems.

A primary characteristic of the nation-state era has been state monopoly of the means of violence. We surely are witnessing—in both Third-Wave/First-World and First-Wave/Third-World societies—a trend away from state monopoly of lethal violence. In a future characterized by cyberwar, technology offers the prospect of non-state possession in abundance of the "non-lethal" means of violence.

Endnotes

1. Alvin and Heidi Toffler, **War and Anti-War: Survival at the Dawn of the 21st Century** (Boston: Little, Brown and Co., 1993).

2. Joseph S. Nye, Jr., and William A. Owens, "America's Information Edge," and Eliot A. Cohen, "A Revolution in Warfare," ***Foreign Affairs***, Vol. 75, No. 2 (March-April) 1996, 20-36 and 37-54, respectively.

3. While the pedigree is difficult to track, it appears that Thomas P. Rona may have coined the term "information war" as early as 1976 in a study written for Boeing Corporation, entitled "Weapons Systems and Information War."

4. George J. Stein, "Information Warfare," in Campen, Dearth, and Goodden (Editors), **Cyberwar: Security, Strategy, and Conflict in the Information Age** (Fairfax, VA: AFCEA International Press, 1996), 175-183.

5. Toffler, particularly 81-85.

6. Chairman of the Joint Chiefs of Staff Instruction 3210.01, 2 January 1996, p. 6. This rather labored definition has replaced the more common-sense 1994 definition: "actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and protecting our information and information systems."

7. See John Arquilla and David Ronfeldt, **Cyberwar Is Coming!**, RAND P-7791, 1992; and Philippe Baumard, "From Info War to Knowledge War: Preparing for the Paradigm Shift," in Campen, Dearth, and Goodden (editors), **Cyberwar: Security, Strategy, and Conflict in the Information Age**, 147-160.

8. Stein, 177.

9. The distinction between the realms espoused by Major General Emory Upton. See Russell F. Weigley, **The American Way of War** (Bloomington: Indiana Univ Press, 1973) 168-171, 221.

10. Toffler, 64-80. The orient, observe, decide, and act (OODA) concept originated with U.S. Air Force Colonel John Boyd in the 1970s.

11. **Information Technologies and the Future of Land Warfare**, RAND Study DDR-659-A, February 1994 (draft).

12. This unfortunate incident was the fault of neither the SEAL Team nor of the waiting journalists. U.S. officials had informed the latter of the landing site. The SEALs apparently did not know that U.S. forces would meet no hostile resistance, and they were following "normal" procedures. The oversight in proper coordination lay with senior planners, who failed to grasp the importance of melding purely military concerns and operations with public diplomacy requirements and activities.

13. RAND DDR-659-A.

14. The literature concerning this phenomenon is voluminous. For one of the best discussions, see Walter B. Wriston, **The Twilight of Sovereignty: How the Information Revolution is Transforming Our World** (New York: Charles Scribner's Sons, 1992).

15. See Winn Schwartau, "Ethical Conundra of Information Warfare," in Campen, Dearth, and Goodden (Eds), **Cyberwar: Security, Strategy, and Conflict in the Information Age**, 243-249.

Mr. Dearth teaches at the Joint Military Intelligence Training Center. A veteran of 25 years in the intelligence business, he has served on the Army War College faculty; as advisor to the Commander, U.S. Special Operations Command; and as Special Assistant to the Executive Director of the Defense Intelligence Agency. Readers can reach Mr. Dearth via E-mail dhdearth@aol.com, and by telephone (202) 231-3290 and DSN 428-3290.

Letters

(Continued from page 7)

tice when the S2 is fully involved and risking his or her own neck by flying cross-FLOT. It shows you have enough confidence in your own analysis to risk your own life, as well as the unit's aircraft and pilots.

Flying in the ATAC keeps the S2 fully apprised of the situation, better then any other intelligence officer in the division or corps. You are there to make those critical assessments as combat information flows in. You can relay critical data to the G2 and save "the weeds" for later. The S2 noncommissioned officer in charge back at the command post is fully capable of monitoring the operations and intelligence nets and passing critical information to you in the ATAC.

Finally, having the S2 fly in the ATAC with the commander or S3 and the fire support officer fuses the staff team. You develop a routine in training and reduce reaction time during actual operations. Remember, the S2 should be "ALWAYS OUT FRONT" and in this case "ABOVE" as well.

Major Stephen K. Iwicki
Washington, D.C.

629th MI Battalion
Maryland National Guard

Oriental blue is the primary branch color of the Military Intelligence Corps. The upper half of the shield alludes to the state flag of Maryland and identifies the home area of the battalion. The panther embodies the established nickname of the unit, "Prowler" and is a predator celebrated for its stealth and patience on the hunt. He is an appropriate symbol for a tactical-level intelligence unit. The lightning flashes refer to the speed of operation and the dominant role of combat electronic warfare on the battlefield.

The 629th MI Battalion of the Maryland Army National Guard is currently the only fully-manned Combat Electronic Warfare Intelligence (CEWI) battalion in the Army National Guard. Composed of a headquarters and headquarters service company, a signals intelligence (SIGINT) collection company, and an interrogation and surveillance company, the battalion provides multidisciplined combat intelligence support to the Commander, 29th Infantry Division (Light).

The 29th ("Blue and Gray") Division was reactivated in the Fall of 1985 as one of five light infantry divisions in the Total Army force structure. The 629th was formed in October 1985, as part of the divisional troops.

The battalion traces its lineage back to the 629th Tank Destroyer Battalion of the World War II-era 29th Infantry Division that stormed Omaha Beach on D-Day. That battalion's insignia, the panther (or "Night Prowler") forms the basis of the insignia displayed above. The lightning bolt clasped in the fangs of the beast signifies the battalion's SIGINT mission, while the motto "Stalk the Prey" is emblematic of the MI mission to continuously seek, find, and never lose the enemy. The colors of the backing shield include the blue of the MI Corps.

Since receiving federal recognition on 3 October 1988, the battalion has established a reputation as the premier Military Intelligence (CEWI) unit in the Reserve Component, with a decade's worth of accomplishments in training arenas and in support of the on-going "real world" needs of the wider intelligence community.

Members of the 629th responded to the call to Operation DESERT SHIELD, providing timely and much-needed support to the 82d Airborne Division and the XVIII Airborne Corps (Rear) efforts in the Continental United States. Members of the command support the National Guard's counternarcotics efforts on a continuing basis, and have supported the efforts of Joint Task Force Six in the American Southwest. The command has been involved in a wide variety of training, and joint exercises such as Ulchi Focus Lens, Atlantic Trail, Reforger, and others.

The 629th MI Battalion is headquartered at Laurel Armory, Laurel, Maryland, in a state-of-the-art facility built for the battalion and officially opened in April 1994. Laurel Armory is also the site of the first of the National Guard's new Distance Learning Network (DLN) centers, featuring the latest in technology in a computer local area network to deliver military occupational specialty courseware, video teleconferencing and training (VTT), and college instruction to National Guardsmen and to the local community.

The 629th MI Battalion (CEWI) is fully-manned and well equipped to answer the nation's call. It continues to provide a viable, vital dimension to the warfighting capabilities of the 29th Light Infantry Division and to the larger missions of America's Army.

Commander
U.S. Army Intelligence Center and Fort Huachuca
ATTN: ATZS-TDL-B (12)
Fort Huachuca, AZ 85613-6000

BULK RATE
U.S. POSTAGE PAID
SIERRA VISTA, AZ
PERMIT NO. 300

Headquarters, Department of the Army.
This publication is approved for public release. Distribution is unlimited.

PIN 075206000